McAfee ePolicy Orchestrator 4.0.2 Product Guide

McAfee®

COPYRIGHT

Copyright © 2008 McAfee, Inc. All Rights Reserved.

No part of this publication may be reproduced, transmitted, transcribed, stored in a retrieval system, or translated into any language in any form or by any means without the written permission of McAfee, Inc., or its suppliers or affiliate companies.

TRADEMARK ATTRIBUTIONS

AVERT, EPO, EPOLICY ORCHESTRATOR, FLASHBOX, FOUNDSTONE, GROUPSHIELD, HERCULES, INTRUSHIELD, INTRUSION INTELLIGENCE, LINUXSHIELD, MANAGED MAIL PROTECTION, MAX (MCAFEE SECURITYALLIANCE EXCHANGE), MCAFEE, MCAFEE.COM, NETSHIELD, PORTALSHIELD, PREVENTSYS, PROTECTION-IN-DEPTH STRATEGY, PROTECTIONPILOT, SECURE MESSAGING SERVICE, SECURITYALLIANCE, SITEADVISOR, THREATSCAN, TOTAL PROTECTION, VIREX, VIRUSSCAN, WEBSHIELD are registered trademarks or trademarks of McAfee, Inc. and/or its affiliates in the US and/or other countries. McAfee Red in connection with security is distinctive of McAfee brand products. All other registered and unregistered trademarks herein are the sole property of their respective owners.

LICENSE INFORMATION

License Agreement

NOTICE TO ALL USERS: CAREFULLY READ THE APPROPRIATE LEGAL AGREEMENT CORRESPONDING TO THE LICENSE YOU PURCHASED, WHICH SETS FORTH THE GENERAL TERMS AND CONDITIONS FOR THE USE OF THE LICENSED SOFTWARE. IF YOU DO NOT KNOW WHICH TYPE OF LICENSE YOU HAVE ACQUIRED, PLEASE CONSULT THE SALES AND OTHER RELATED LICENSE GRANT OR PURCHASE ORDER DOCUMENTS THAT ACCOMPANIES YOUR SOFTWARE PACKAGING OR THAT YOU HAVE RECEIVED SEPARATELY AS PART OF THE PURCHASE (AS A BOOKLET, A FILE ON THE PRODUCT CD, OR A FILE AVAILABLE ON THE WEB SITE FROM WHICH YOU DOWNLOADED THE SOFTWARE PACKAGE). IF YOU DO NOT AGREE TO ALL OF THE TERMS SET FORTH IN THE AGREEMENT, DO NOT INSTALL THE SOFTWARE. IF APPLICABLE, YOU MAY RETURN THE PRODUCT TO MCAFEE OR THE PLACE OF PURCHASE FOR A FULL REFUND.

License Attributions

Refer to the product Release Notes.

Contents

Introducing ePolicy Orchestrator 4.0.2 . . . . . **13**

ePolicy Orchestrator 4.0.2 components and what they do. 13

The ePO server. 13

The McAfee Agent. 14

Using this guide. 14

Audience. 15

Where to find McAfee enterprise product information. 15

Configuring ePolicy Orchestrator Servers **16**

ePO user accounts. 17

Global administrators. 17

How permission sets work. 17

Contacts. 18

Server settings and the behaviors they control. 18

Available server tasks and what they do. 19

The Audit Log. 20

The Event Log. 20

Data exports from any table or chart. 21

MyAVERT Security Threats 22

Logging on and off from ePO servers. 22

Logging on to ePO servers. 22

Logging off of ePO servers. 23

Viewing the server version number 23

Working with user accounts. 23

Creating user accounts. 23

Editing user accounts. 24

Deleting user accounts. 24

Working with permission sets. 24

Creating permission sets for user accounts. 25

Duplicating permission sets. 25

Editing permission sets. 26

Deleting permission sets. 26

Working with contacts. . . . 26
Creating contacts. . . . 26
Editing contacts. . . . 27
Deleting contacts. . . . 27
Working with server settings. . . . 27
Specifying an email server. . . . 28
Configuring the template and location for exported reports. . . . 28
Determining which events are forwarded to the server. . . . 28
Viewing and changing communication ports. . . . 29
Working with the Server Task Log. . . . 29
Viewing the Server Task Log. . . . 30
Filtering the Server Task Log. . . . 30
Purging the Server Task Log. . . . 31
Working with the Audit Log. . . . 31
Viewing the Audit Log. . . . 31
Purging the Audit Log. . . . 32
Purging the Audit Log on a schedule. . . . 32
Working with the Event Log. . . . 33
Viewing the Event Log. . . . 33
Purging events. . . . 33
Purging the Event Log on a schedule. . . . 34
Working with MyAvert Security Threats. . . . 34
Configuring MyAvert update frequency and proxy settings. . . . 35
Viewing threat notifications. . . . 35
Deleting threat notifications. . . . 35
Exporting tables and charts to other formats. . . . 36
Allowed Cron syntax when scheduling a server task. . . . 36

Organizing Systems for Management. . . . 38

The System Tree. . . . 39
Considerations when planning your System Tree. . . . 40
Administrator access. . . . 40
Environmental borders and their impact on system organization. . . . 41
Subnets and IP address ranges. . . . 41
Tags and systems with similar characteristics. . . . 42
Operating systems and software. . . . 42
Tags and how they work. . . . 42
Active Directory and NT domain synchronization. . . . 43

Active Directory synchronization. . . . 43
NT domain synchronization. . . . 45
Criteria-based sorting. . . . 45
How settings affect sorting. . . . 46
IP address sorting criteria. . . . 46
Tag-based sorting criteria. . . . 47
Group order and sorting. . . . 47
Catch-all groups. . . . 47
How a system is first placed in the System Tree. . . . 47
Working with tags. . . . 48
Creating tags with the Tag Builder. . . . 49
Excluding systems from automatic tagging. . . . 49
Applying tags to selected systems. . . . 50
Applying criteria-based tags automatically to all matching. . . . 50
Creating and populating groups. . . . 51
Creating groups manually. . . . 52
Adding systems manually to an existing group. . . . 53
Importing systems from a text file. . . . 54
Sorting systems into criteria-based groups. . . . 55
Importing Active Directory containers. . . . 57
Importing NT domains to an existing group. . . . 59
Synchronizing the System Tree on a schedule. . . . 61
Updating the synchronized group with an NT domain manually. . . . 62
Moving systems manually within the System Tree. . . . 62
Distributing Agents to Manage Systems. . . . 64
Agents and SuperAgents. . . . 65
Agent-server communication 66
SuperAgents and broadcast wake-up calls. . . . 67
Agent activity logs. . . . 69
Agent policy settings. . . . 69
Security Keys. . . . 71
Agent-server secure communication keys. . . . 71
Master repository key pair. . . . 72
Other repository public keys. . . . 72
Methods of agent distribution. . . . 72
Creating custom agent installation packages. . . . 73
Distributing agents. . . . 73

Deploying the agent with ePolicy Orchestrator. . . . 74
Installing the agent with login scripts. . . . 76
Installing the agent manually. . . . 77
Enabling the agent on unmanaged McAfee products. . . . 78
Including the agent on an image. . . . 78
Using other deployment products. . . . 79
Distributing the agent to WebShield appliances and Novell NetWare servers. . . . 79
Forcing the agent to call in to the server. . . . 79
Upgrading existing agents. . . . 79
Upgrading agents using login scripts or manual installation. . . . 80
Upgrading agents with ePolicy Orchestrator. . . . 80
Removing the agent. . . . 81
Running FRMINST.EXE from a command line. . . . 81
Removing agents when deleting systems from the System Tree. . . . 81
Removing agents when deleting groups from the System Tree. . . . 82
Removing agents from systems in query results. . . . 82
Maintaining the agent. . . . 82
Sending manual wake-up calls to systems. . . . 83
Sending manual wake-up calls to a group. . . . 83
Sending wake-up calls on a schedule. . . . 84
Viewing the agent activity log. . . . 85
Viewing of the agent and product properties. . . . 85
Running agent tasks from the managed system. . . . 86
Working with security keys. . . . 88
Agent command-line options. . . . 94
Agent installation command-line options. . . . 94
Creating Repositories. . . . 96
Repository types and what they do. . . . 96
Types of distributed repositories. . . . 98
Repository branches and their purposes. . . . 99
Repository list file and its uses. . . . 99
How repositories work together. . . . 100
Ensuring access to the source site. . . . 101
Using Internet Explorer proxy settings for the master repository. . . . 101
Configuring custom proxy settings for the master repository 102
Working with source and fallback sites. . . . 103
Switching source and fallback sites. . . . 103

Creating source sites. . . . 104
Editing source and fallback sites. . . . 105
Deleting source or fallback sites. . . . 105
Using SuperAgents as distributed repositories. . . . 105
Creating SuperAgent repositories. . . . 106
Selecting which packages are replicated to SuperAgent repositories. . . . 106
Deleting SuperAgent distributed repositories. . . . 107
Creating and configuring FTP, HTTP, and UNC repositories. . . . 107
Creating a folder location on an FTP, HTTP server or UNC share. . . . 108
Adding the distributed repository to ePolicy Orchestrator. . . . 108
Enabling folder sharing for UNC and HTTP repositories. . . . 109
Editing distributed repositories 110
Deleting distributed repositories. . . . 110
Working with the repository list files. . . . 110
Exporting the repository list SITELIST.XML file. . . . 110
Exporting the repository list SITEMGR.XML file for backup or use by other servers. . . . 111
Importing distributed repositories from the SITEMGR.XML file. . . . 111
Importing source sites from the SITEMGR.XML file. . . . 112
Changing credentials on multiple distributed repositories. . . . 112
Managing Products with Policies and Client Tasks. . . . 114
Extensions and what they do. . . . 114
Policy management. . . . 115
Policy application. . . . 116
Client tasks and what they do. . . . 117
Bringing products under management. . . . 118
Viewing policy information. . . . 118
Viewing groups and systems where a policy is assigned. . . . 118
Viewing the settings of a policy. . . . 119
Viewing policy ownership. . . . 119
Viewing assignments where policy enforcement is disabled. . . . 119
Viewing policies assigned to a group. . . . 120
Viewing policies assigned to a specific system. . . . 120
Viewing a group's policy inheritance. . . . 120
Viewing and resetting broken inheritance. . . . 120
Working with the Policy Catalog. . . . 121
Creating a policy on the Policy Catalog page 121
Duplicating a policy on the Policy Catalog page. . . . 122

Editing a policy's settings from the Policy Catalog. . . . 122
Renaming a policy from the Policy Catalog. . . . 122
Deleting a policy from the Policy Catalog. . . . 123
Working with policies. . . . 123
Changing the owner of a policy. . . . 123
Sharing policies between ePO servers. . . . 124
Assigning a policy to a group of the System Tree. . . . 125
Assigning a policy to a managed system. . . . 125
Assigning a policy to multiple managed systems within a group. . . . 126
Enforcing policies for a product on a group. . . . 126
Enforcing policies for a product on a system. . . . 126
Copying and pasting assignments. . . . 127
Working with client tasks. . . . 128
Creating and scheduling client tasks. . . . 129
Editing client tasks. . . . 129
Deleting client tasks. . . . 129
Frequently asked questions. . . . 130
Deploying Software and Updates. . . . 131
Deployment packages for products and updates. . . . 131
Product and update deployment. . . . 133
Deployment tasks. . . . 134
Update tasks. . . . 134
Global updating. . . . 135
Pull tasks. . . . 136
Replication tasks. . . . 137
Repository selection. . . . 137
Server Task Log. . . . 138
Checking in packages manually. . . . 138
Using the Product Deployment task to deploy products to managed systems. . . . 139
Configuring the Deployment task for groups of managed systems. . . . 140
Configuring the Deployment task to install products on a managed system. . . . 140
Deploying update packages automatically with global updating. . . . 141
Deploying update packages with pull and replication tasks. . . . 142
Using pull tasks to update the master repository. . . . 143
Replicating packages from the master repository to distributed repositories. . . . 145
Configuring agent policies to use a distributed repository. . . . 147
Using local distributed repositories that are not managed. . . . 147

Checking in engine, DAT and EXTRA.DAT update packages manually. 148
Updating managed systems regularly with a scheduled update task. 149
Confirming that clients are using the latest DAT files. 149
Evaluating new DATs and engines before distribution. 150
Manually moving DAT and engine packages between branches. 150
Deleting DAT or engine packages from the master repository. 151

Sending Notifications **152**

Notifications and how it works. 153
Throttling and aggregation. 153
Notification rules and System Tree scenarios. 153
Default rules. 155
Planning. 155
Determining how events are forwarded. 156
Determining which events are forwarded immediately. 156
Determining which events are forwarded. 157
Setting up ePO Notifications. 157
Giving users appropriate permissions to Notifications. 157
Working with SNMP servers. 158
Working with registered executables and external commands. 160
Creating and editing Notification rules. 163
Describing the rule. 163
Setting filters for the rule. 164
Setting thresholds of the rule. 164
Configuring the notifications for the rule. 165
Viewing the history of Notifications. 166
Configuring the Notification Log. 166
Viewing the details of Notification Log entries. 167
Purging the Notifications Log. 167
Product and component list. 168
Frequently asked questions. 168

Querying the Database **170**

Queries. 170
Public and personal queries. 171
Query permissions. 171
Query Builder. 172
Multi-server roll-up querying. 173
Preparing for roll-up querying. 174

Registering ePO servers. . . . 174
Creating a Data Roll Up server task. . . . 174
Working with queries. . . . 175
Creating custom queries. . . . 175
Running an existing query. . . . 176
Running a query on a schedule. . . . 176
Making personal queries public. . . . 178
Duplicating queries. . . . 178
Sharing a query between ePO servers. . . . 179
Exporting query results to other formats. . . . 179
Default queries and what they display. . . . 180
MA: Agent Communication Summary query. . . . 180
MA: Agent Version Summary query. . . . 180
ePO: Compliance History query. . . . 181
ePO: Compliance Summary query. . . . 181
ePO: Malware Detection History query. . . . 181
ePO: Distributed Repository Status query. . . . 182
ePO: Failed User Actions in ePO Console query. . . . 182
ePO: Failed Logon Attempts query. . . . 182
ePO: Multi-Server Compliance History query. . . . 182
ePO: Systems per Top-Level Group query. . . . 183
ePO: Systems Tagged as Server query. . . . 183
ePO: Today's Detections per Product query. . . . 183

Assessing Your Environment With Dashboards. . . . 184

Dashboards and how they work. . . . 184
Queries as dashboard monitors. . . . 184
Default dashboard monitors. . . . 184
Setting up dashboard access and behavior. . . . 185
Giving users permissions to dashboards. . . . 185
Configuring the refresh frequency of dashboards. . . . 185
Working with Dashboards. . . . 186
Creating dashboards. . . . 186
Making a dashboard active. . . . 186
Selecting all active dashboards. . . . 187
Making a dashboard public. . . . 187

Detecting Rogue Systems. . . . 189

What are rogue systems. . . . 189

How the Rogue System Sensor works. . . . 190
Passive listening to layer-2 traffic. . . . 190
Intelligent filtering of network traffic. . . . 190
Data gathering and communications to the server. . . . 191
Systems that host sensors. . . . 191
How detected systems are matched and merged. . . . 192
Rogue System Detection states. . . . 192
Overall system status. . . . 193
Rogue System Sensor status. . . . 194
Subnet status. . . . 195
Top 25 Subnets. . . . 195
Rogue Sensor Blacklist. . . . 195
Rogue System Detection policy settings. . . . 196
Considerations for policy settings. . . . 196
Rogue System Detection permission sets. . . . 197
Setting up Rogue System Detection. . . . 198
Configuring Rogue System Detection policy settings. . . . 198
Configuring server settings for Rogue System Detection. . . . 199
Editing compliance settings. . . . 199
Editing matching settings. . . . 199
Editing sensor settings. . . . 200
Setting up automatic responses to Rogue System Detection events. . . . 201
Working with detected systems. . . . 202
Adding systems to the Exceptions list. . . . 202
Adding systems to the Rogue Sensor Blacklist. . . . 202
Editing system comments. . . . 203
Exporting the Exceptions list. . . . 203
Importing systems to the Exceptions list. . . . 204
Merging detected systems. . . . 204
Removing systems from the Detected Systems list. . . . 204
Removing systems from the Exceptions list. . . . 205
Removing systems from the Rogue Sensor Blacklist. . . . 205
Viewing detected systems and their details. . . . 206
Working with sensors. . . . 206
Changing the sensor-to-server port number. . . . 206
Installing sensors. . . . 207
Editing sensor descriptions. . . . 208

Removing sensors. . . . 209
Working with subnets. . . . 210
Adding subnets. . . . 210
Deleting subnets. . . . 210
Ignoring subnets. . . . 211
Including subnets. . . . 211
Renaming subnets. . . . 211
Viewing detected subnets and their details. . . . 212
Rogue System Detection command-line options. . . . 212
Default Rogue System Detection queries. . . . 213
Appendix: Maintaining ePolicy Orchestrator databases. . . . 214
Performing daily or weekly database maintenance. . . . 214
Performing weekly maintenance of MSDE databases. . . . 214
Performing regular maintenance of SQL Server databases. . . . 215
Backing up ePolicy Orchestrator databases regularly. . . . 216
Backing up a SQL database--see your SQL documentation. . . . 216
Backing up an MSDE database. . . . 216
Changing SQL Server information. . . . 217
Restoring ePolicy Orchestrator databases. . . . 217
Restoring a SQL database--see your SQL documentation. . . . 218
Restoring an MSDE database from a backup. . . . 218

Introducing ePolicy Orchestrator 4.0.2

ePolicy Orchestrator 4.0.2 provides a scalable platform for centralized policy management and enforcement of your security products and the systems on which they reside. It also provides comprehensive reporting and product deployment capabilities, all through a single point of control.

Contents

- ePolicy Orchestrator 4.0.2 components and what they do
- Using this guide
- Where to find McAfee enterprise product information

ePolicy Orchestrator 4.0.2 components and what they do

The ePolicy Orchestrator software is comprised of these components:

- ePO server — The center of your managed environment. The server delivers security policy and tasks, controls updates, and processes events for all managed systems.
- Master repository — The central location for all McAfee updates and signatures, residing on the ePO server. Master repository retrieves user-specified updates and signatures from McAfee or user-defined source sites.
- Distributed repositories — Placed strategically throughout your environment to provide access for managed systems to receive signatures, product updates, and product installations with minimal bandwidth impact. Depending on how your network is set up, you can set up SuperAgent, HTTP, FTP, or UNC share distributed repositories.
- McAfee Agent — A vehicle of information and enforcement between the ePO server and each managed system. The agent retrieves updates, ensures task implementation, enforces policies and forwards events for each managed system.

The ePO server

The ePO server provides management, reporting, and enforcement capabilites and includes:

- A robust database that accrues information about product operation on the client systems in your network.
- A querying system that lets you monitor the security status in your company, and quickly act on gathered data.
- A software repository that stores the products and product updates (for example, DAT files) that you deploy to your network.

The ePolicy Orchestrator server can segment the user population into discrete groups for customized policy management. Each server can manage up to 250,000 systems.

The McAfee Agent

The agent is installed on the systems you intend to manage with ePolicy Orchestrator.

While running silently in the background, the agent:

- Gathers information and events from managed systems and sends them to the ePolicy Orchestrator server.
- Installs products and updates on managed systems.
- Enforces policies and tasks on managed systems and sends events back to the ePO server.

You can deploy the agent from the console (to Windows systems) or copy the agent installation package onto removable media or into a network share for manual or login script installation on your systems. Agents must be installed manually on UNIX systems.

Using this guide

This guide provides information on configuring and using your product. For system requirements and installation instructions, see the *Installation Guide*.

This material is organized in the order that McAfee recommends to set up ePolicy Orchestrator in a production environment for the first time, and is also accessible to anyone seeking specific topics.

Setting up ePolicy Orchestrator for the first time?

This guide serves as a tool to help administrators set up their ePolicy Orchestrator environment for the first time, and as a reference tool for more experienced users. Depending on your environment, you may perform some of these tasks in a slightly different order.

McAfee recommends setting up ePolicy Orchestrator for the first time in this order:

1. Configure ePolicy Orchestrator servers — Set up user accounts and permissions, configure settings, and get familiar with the user interface.
2. Organize systems for management — The System Tree allows you to organize and act on all systems you manage with ePolicy Orchestrator. Before setting up other features, you must create your System Tree.
3. Distribute agents — Each system you want to manage must have the McAfee Agent installed. This section provides detailed information on distributing and maintaining agents in your environment.
4. Create repositories — Before deploying any products, components, or updates to your managed systems with ePolicy Orchestrator, you must configure and create update repositories.
5. Manage product policies and tasks — Before deploying any products, components, or updates to your managed systems with ePolicy Orchestrator, McAfee recommends configuring the policy settings for these products and components. Although it is not required to configure policy settings before deployment, by doing so you can ensure that the products and components have the desired settings as soon as possible.

6 Deploy software and updates — Once your update repositories and policy settings are created and configured, deploy the products, components, and updates to the desired systems with ePolicy Orchestrator.

7 Configure advanced features — Once your managed environment is up and running, you can configure and implement ePolicy Orchestrator's advanced features, like Notifications, queries and dashboards.

Audience

This information is intended primarily for network administrators who are responsible for their company's security program, and assumes the customer has installed and used ePolicy Orchestrator in a lab environment.

Where to find McAfee enterprise product information

The McAfee documentation is designed to provide you with the information you need during each phase of product implementation, from evaluating a new product to maintaining existing ones. Depending on the product, additional documents might be available. After a product is released additional information regarding the product is entered into the online Knowledgebase available on McAfee ServicePortal.

Evaluation Phase	Installation Phase	Setup Phase	Maintenance Phase
How can my company benefit from this product? *Evaluation Tutorial* • Preparing for, installing and deploying software in a test environment. • Detailed instructions for common tasks.	Before, during, and after installation. *Release Notes* • Known issues in the current release. • Issues resolved since the last release. • Last-minute changes to the product or its documentation. *Installation Guide* • Preparing for, installing and deploying software in a production environment.	Getting up-and-running with the product. *Product Guide* and *Online Help* • Setting up and customizing the software for your environment. *Online Help* • Managing and deploying products through ePolicy Orchestrator. • Detailed information about options in the product.	Maintaining the software. *Online Help* • Maintaining the software. • Reference information. • All information found in the product guide. *Quick Reference Card* • Detailed instructions for common and infrequent important tasks. *Knowledgebase* (knowledge.mcafee.com) • Release notes and documentation. • Supplemental product information. • Workarounds to known issues.

Finding release notes and documentation for McAfee enterprise products

1 Go to knowledge.mcafee.com and select **Product Documentation** under **Useful links**.

2 Select **<Product Name>** | **<Product Version>** and select the required document from the list of documents.

Configuring ePolicy Orchestrator Servers

The ePO server is the center of your managed environment, providing a single location from which to administer system security throughout your network.

If your organization is very large or divided into multiple large sites, consider installing a separate server at each site. This can reduce network traffic when managing agents, sending updates, and replicating to distributed repositories within a local LAN. Network traffic has a larger impact on your resources when this communication takes place across WAN, VPN, or other slower network connections typically found between remote sites.

Are you configuring the ePO server for the first time?

When configuring the ePO server for the first time:

1. Review the conceptual information on user accounts, permission sets, server settings and server tasks.
2. Decide on how to implement the flexibility of permission sets with user accounts.
3. Create user accounts and permission sets, and assign the permission sets as needed.
4. Set up your contacts list and email server settings.

Contents

- ePO user accounts
- How permission sets work
- Contacts
- Server settings and the behaviors they control
- Available server tasks and what they do
- The Audit Log
- The Event Log
- Data exports from any table or chart
- MyAVERT Security Threats
- Logging on and off from ePO servers
- Viewing the server version number
- Working with user accounts
- Working with permission sets
- Working with contacts
- Working with server settings
- Working with the Server Task Log
- Working with the Audit Log

- Working with the Event Log
- Working with MyAvert Security Threats
- Exporting tables and charts to other formats
- Allowed Cron syntax when scheduling a server task

ePO user accounts

User accounts provide a means for users to access and use the software. They are associated with permission sets, which define what users are allowed to do with the software.

You must create user accounts and permission sets to accommodate the needs of each user that logs on to the ePO server.

There are two types of users, global administrators and everyone else.

Global administrators

Global administrators have read and write permissions and rights to all operations. When you install the server a global administrator account with the user name admin is created.

You can create additional global administrator accounts for people who require global administrative rights.

Permissions exclusive to global administrators include:

- Create, edit, and delete source and fallback sites.
- Change server settings.
- Add and delete user accounts.
- Add, delete, and assign permission sets.
- Import events into ePolicy Orchestrator databases and limit events that are stored there.

How permission sets work

A permission set is a group of permissions that can be granted to any users by assigning it to those users' accounts. One or more permission sets can be assigned to any users who are not global administrators (global administrators have all permissions to all products and features).

Permission sets only grant rights and access — no permission ever removes rights or access. When multiple permission sets are applied to a user account, they aggregate. For example, if one permission set does not provide any permissions to server tasks, but another permission set applied to the same account grants all permissions to server tasks, that account has all permissions to server tasks. Consider this as you plan your strategy for granting permissions to the users in your environment.

When are permission sets assigned?

Global administrators can assign existing permission sets when creating or editing user accounts and when creating or editing permission sets.

What happens when I install new products?

When a new product extension is installed it may add one or more groups of permissions to the permission sets. For example, when you install a VirusScan Enterprise extension, a VirusScan Enterprise section is added to each permission set. Initially, the newly added section is listed in each permission set with no permissions yet granted. The global administrators can then grant permissions to users through existing or new permission sets.

Default permission sets

ePolicy Orchestrator 4.0.2 ships with four default permission sets that provide permissions to ePolicy Orchestrator functionality. These are:

- Executive Reviewer — Provides view permissions to dashboards, events, contacts, and can view information that relates to the entire System Tree.
- Global Reviewer — Provides view access globally across functionality, products, and the System Tree, except for extensions, multi-server roll-up data, registered servers, and software.
- Group Admin — Provides view and change permissions across ePolicy Orchestrator features. Users that are assigned this permission set each need at least one more permission set that grants access needed products and groups of the System Tree.
- Group Reviewer — Provides view permissions across ePolicy Orchestrator features. Users that are assigned this permission set each need at least one more permission set that grants access needed products and groups of the System Tree.

Contacts

Maintain a list of email addresses that ePolicy Orchestrator uses to send email messages to specified users in response to events. Currently this list is used by Notifications, queries, and export functionality.

Server settings and the behaviors they control

Various settings control how the ePolicy Orchestrator server behaves. You can change most settings at anytime. However, you must reinstall the software to change the name of the server or the port number the server uses for HTTP communication.

Types of ePO server settings are:

- Email server — Sepcifies the email server that is used when ePolicy Orchestrator sends email messages.
- Event Filtering — Specifies which events are forwarded by the agent.
- Global Updating — Specifies whether and how global updating is enabled.
- MyAvert Security Threats — Specifies proxy settings and the update frequency for the MyAvert Security Threats service.
- Ports — Specifies the ports used by the server when communicating with agents and the database.
- Printing and exporting — Specifies how information is exported to other formats, and the template for PDF exports.

- Repository Packages — Specifies whether any package can be checked in to any branch. Only agents later then version 3.6 can retrieve packages other than updates from branches other than Current.
- Security Keys — Specifies and manages the agent-server secure communication keys, repository keys.
- System Tree Sorting — Specifies whether and how System Tree sorting is enabled in your environment.

Available server tasks and what they do

The default set of server tasks is described here. For details on each of these, see the appropriate section of this guide that covers that server task.

Improvements to server tasks

Server tasks are now more configurable, allowing you to chain multiple actions and subactions within a single task, as well as more flexible scheduling.

Server task actions

- Event Migration — If you upgrade from a previous ePolicy Orchestrator installation, use this task to migrate events from the old database to the new database, so that you can run queries against your historical data. McAfee recommends scheduling this task to run at off hours as soon as you can after upgrading.
- NT Domain/Active Directory Synchronization — Synchronizes select Windows NT domains and Active Directory containers that are mapped to System Tree groups. This task can also be performed manually.
- Purge Audit Log — Deletes entries from the Audit Log on user-configured age.
- Purge Event Log — Deletes events from the database based on user-configured criteria.
- Purge Notification Log — Deletes entries from the Notification Log by user-configured time.
- Purge Server Task Log — Deletes entries from the Server Task Log by user-configured age.
- Repository Pull — Retrieves packages from the source site, then places them in the master repository.
- Repository Replication — Updates distributed repositories from the master repository.
- Roll Up Data: Managed Systems— Imports summary data from other registered ePO servers.
- Roll Up Data: Compliance History — Imports summary compliance data from other registered ePO servers.
- Run Query — Runs a selected query and allows you to chain subactions related to the query results. For example, you can email the results to someone in your organization, or deploy agents to all systems in the query results.
- Run Tag Criteria — Evaluates all managed systems against a selected tag's criteria, and applies the tag to all matching systems.

The Audit Log

Use the Audit Log to maintain and access a record of all ePO user actions. The Audit Log entries display in a sortable table. For added flexibility, you can also filter the log so that it only displays failed actions, or only entries that are within a certain age.

The Audit Log displays seven columns:

- **Action** — The name of the action the ePO user attempted.
- **Completion Time** — The time the action finished.
- **Details** — More information about the action.
- **Priority** — Importance of the action.
- **Start Time** — The time the action was initiated.
- **Success** — Specifies whether the action was successfully completed.
- **User Name** — User name of the logged-on user account that was used to take the action.

Audit Log entries can be queried against. You can create queries with the Query Builder wizard that target this data, or you can use the default queries that target this data. For example, the **Failed Logon Attempts** query retrieves a table of all failed logon attempts.

The Event Log

Use the Event Log to quickly view and sort through events in the database. The Event Log can be purged only by age.

You can choose which columns are displayed in the sortable table. You can choose from a variety of event data to use as columns.

Depending on which products you are managing, you can also take certain actions on the events. Actions are available on the buttons at the bottom of the page.

Common event format

All managed products now use a common event format. The fields of this format can be used as columns in the Event Log. These include:

- Action Taken — The action that was taken by the product in response to the threat.
- Agent GUID — Unique identifier of the agent that forwarded the event.
- DAT Version — DAT version on the system which sent the event.
- Detecting Product Host Name — Name of the system hosting hosting the detecting product.
- Detecting Product ID — ID of the detecting product.
- Detecting Product IPv4 Address — IPv4 address of the system hosting the detecting product (if applicable).
- Detecting Product IPv6 Address — IPv6 address of the system hosting the detecting product (if applicable).
- Detecting Product MAC Address — MAC address of the system hosting the detecting product.
- Detecting Product Name — Name of the detecting managed product.
- Detecting Product Version — Version number of the detecting product.

- Engine Version — Version number of the detecting product's engine (if applicable).
- Event Category — Category of the event. Possible categories depend on the product.
- Event Generated Time (UTC) — Time in Coordinated Universal Time that the event was detected.
- Event ID — Unique identifier of the event.
- Event Received Time (UTC) — Time in Coordinated Universal Time that the event was received by the ePO server.
- File Path
- Host Name — Name of the system which sent the event.
- IPv4 Address — IPv4 address of the system which sent the event.
- IPv6 Address — IPv6 address of the system which sent the event.
- MAC Address — MAC address of the system which sent the event.
- Network Protocol — The threat target protocol for network-homed threat classes.
- Port Number — The threat target port for network-homed threat classes.
- Process Name — The target process name (if applicable).
- Server ID
- Threat Name — Name of the threat.
- Threat Source Host Name — System name from which the threat originated.
- Threat Source IPv4 Address — IPv4 address of the system from which the threat originated.
- Threat Source IPv6 Address — IPv6 address of the system from which the threat originated.
- Threat Source MAC Address — MAC address of the system from which the threat originated.
- Threat Source URL — URL from which the threat originated.
- Threat Source User Name — User name from which the threat originated.
- Threat Type — Class of the threat.
- User Name — The threat source user name or email address.

Data exports from any table or chart

Data in any chart or table in ePolicy Orchestrator can be exported to four different formats. Exported results are historical data and are not refreshed.

Unlike query results in the console, data in exported reports is not actionable.

Reports are available in several formats:

- CSV — Use this format to use the data in a spreadsheet application (for example, Microsoft Excel).
- XML — Use this format to transform the data for other purposes.
- HTML — Use this report format to view the exported results as a web page.
- PDF — Use this report format when you need to print the results.

Exported data can be named and saved to any location, or emailed as attachments.

MyAVERT Security Threats

The **MyAvert Security Threats** page informs you of the top ten medium-to-high-risk threats for corporate users. You no longer need to manually search for this information from the press (TV, radio, newspapers), informational web sites, mailing lists, or your peers. You are automatically notified of these threats from McAfee Avert.

Protection status and risk assessment

You can easily determine whether the DAT and engine files in the Current branch of the master repository provide protection against the top ten threats and, if not, the highest risk level of any new threats.

Protection available

The DAT and engine files in the repository already provide protection against all threats that are known to Avert. To determine whether each managed system is protected run a query against DAT and engine file coveraget.

Protection pending on Mediium-to-Low Risk Threats

The updated DAT file for threats assessed by AVERT as medium risk is pending. However, updated protection is available in a supplemental virus definition (EXTRA.DAT) file, which you can manually download if you need protection before the next full DAT file is available, such as in an outbreak scenario.

Protection Pending on High-Risk Threats

The updated DAT file for threats assessed by AVERT as high risk is pending. However, updated protection is available in a supplemental virus definition (EXTRA.DAT) file, which you can manually download if you need protection before the next full DAT file is available, such as in an outbreak scenario.

Logging on and off from ePO servers

Use these tasks to log on to and off from ePO servers. Before using ePolicy Orchestrator, you must be logged on to the ePO server with valid account credentials.

Tasks

- Logging on to ePO servers
- Logging off of ePO servers

Logging on to ePO servers

Use this task to log on to the ePO server. You must have valid credentials to do this. You can log on to multiple ePO servers by opening a new browser session for each ePO server.

Task

1 Open an Internet browser and go to the URL of the server. The **Log On to ePolicy Orchestrator** dialog box appears.

2 Type the **User name** and **Password** of a valid account.

NOTE: Passwords are case-sensitive.

3 Select the **Language** you want the software to display.

4 Click **Log On**.

Logging off of ePO servers

Use this task to log off of ePO servers. Log off from the ePO server whenever you finish using the software.

Task

- To log off from the server, click **Log Off** at the top of any page, or close the browser.

Viewing the server version number

You can view the version number, edition, and license information of the ePolicy Orchestrator server.

- To view the version number, edition, log on to the desired ePolicy Orchestrator server. This information appears in the title bar.
- To view license information, go to the logon page.
- To view extension version information, go to **Configuration | Extension**.

Working with user accounts

Use these tasks to create and maintain user accounts.

Tasks

▸ Creating user accounts
▸ Editing user accounts
▸ Deleting user accounts

Creating user accounts

Use this task to create a user account. You must be a global administrator to add, edit, or delete user accounts.

Task

For option definitions, click **?** on the page displaying the options.

1 Go to **Configuration | Users**.

2 Click **New User**. The **New User** page appears.

3 Type a user name.

4 Select whether to enable or disable the logon status of this account. If this account is for someone who is not yet a part of the organization you may want to disable it.

5 Select whether the new account uses **ePO authentication** or **Windows authentication**, and provide the required credentials.

6 Optionally, provide the user's full name, email address, phone number, and a description in the **Notes** text box.

7 Choose to make the user a global administrator, or select the desired permission sets for the user.

8 Click **Save** to save the current entries and return to the **Users** tab. The new user should appear in the **Users** list.

Editing user accounts

Use this task to edit a user account. Global administrators can change passwords on any user account. Other users can only change passwords on their own accounts.

Task

For option definitions, click **?** on the page displaying the options.

1 Go to **Configuration | Users**.

2 Select the user you want to edit in the **Users** list, then click **Edit**.

3 Edit the account as needed.

4 Click **Save**.

Deleting user accounts

Use this task to delete a user account. You must be a global administrator to delete user accounts.

NOTE: McAfee recommends disabling the **Login status** of an account instead of deleting it until you are sure all valuable information associated with the account has been moved to other users.

Task

For option definitions, click **?** on the page displaying the options.

1 Go to **Configuration | Users**.

2 Select the user you want to delete in the **Users** list, then click **Delete**.

3 Click **OK**.

Working with permission sets

Use these tasks to create and maintain permission sets.

Tasks

- Creating permission sets for user accounts
- Duplicating permission sets

- Editing permission sets
- Deleting permission sets

Creating permission sets for user accounts

Use this task to create a permission set.

Before you begin

You must be a global administrator to perform this task.

Task

For option definitions, click **?** on the page displaying the options.

1 Go to **Configuration | Permission Sets**, then click **New Permission Set**.

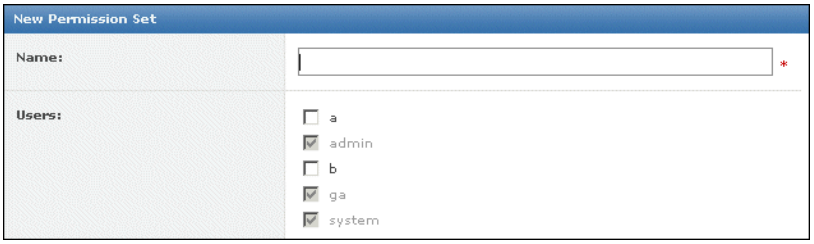

Figure 1: New Permission Set page

2 Type a name for the permission set and select the users to which the set is assigned.

3 Click **Save**. The **Permission Sets** page appears.

4 Select the new permission set from the **Permission Sets** list. Its details appear to the right.

5 Click **Edit** next to any section from which you want to grant permissions.

6 On the **Edit Permission Set** page that appears, select the appropriate options, then click **Save**.

7 Repeat for all desired sections of the permission set.

Duplicating permission sets

Use this task to duplicate a permission set. Only global administrators can duplicate permission sets.

Task

For option definitions, click **?** on the page displaying the options.

1 Go to **Configuration | Permission Sets**, then select the permission set you want to edit in the **Permission Sets** list. Its details appear to the right.

2 Click **Duplicate**, type a **New name** in the **Action** pane, then click **OK**.

3 Select the new duplicate in the **Permission Sets** list. Its details appear to the right.

4 Click **edit** next to any section with which you want to grant permissions.

5 On the **Edit Permission Set** page that appears, select the appropriate options, then click **Save**.

6 Repeat for all sections of the permission set with which you want to grant permissions.

Editing permission sets

Use this task to edit a permission set. Only global administrators can edit permission sets.

Task

For option definitions, click **?** on the page displaying the options.

1. Go to **Configuration | Permission Sets**, then select the permission set you want to edit in the **Permission Sets** list. Its details appear to the right.
2. Click **Edit** next to any section from which you want to grant permissions.
3. On the **Edit Permission Set** page that appears, select the appropriate options, then click **Save**.
4. Repeat for all desired sections of the permission set.

Deleting permission sets

Use this task to delete a permission set. Only global administrators can delete permission sets.

Task

For option definitions, click **?** on the page displaying the options.

1. Go to **Configuration | Permission Sets**, then select the permission set you want to delete in the **Permission Sets** list. Its details appear to the right.
2. Click **Delete**, then click **OK** in the **Action** pane. The permission set no longer appears in the **Permission Sets** list.

Working with contacts

Use these tasks to create and maintain email address information of individuals that may receive email messages from ePolicy Orchestrator.

Tasks

- Creating contacts
- Editing contacts
- Deleting contacts

Creating contacts

Use this task to add email addresses to Contacts.

Task

For option definitions, click **?** on the page displaying the options.

1 Go to **Configuration | Contacts**, then click **New Contact**.

Figure 2: New Contact page

2 Type a first name, last name, and email address for the contact.

3 Click **Save**. The new contact appears on the **Contacts** page.

Editing contacts

Use this task to edit information in an existing entry on the **Contacts** page.

Task

For option definitions, click **?** on the page displaying the options.

1 Go to **Configuration | Contacts**, then select a contact.

2 Click **Edit**. The **Edit Contact** page appears.

3 Edit the information as desired.

4 Click **Save**.

Deleting contacts

Use this task to delete entries from the **Contacts** page.

Task

For option definitions, click **?** on the page displaying the options.

1 Go to **Configuration | Contacts**, then select a contact.

2 Click **Delete**, then click **OK** in the **Action** pane. The contact no longer appears in the list.

Working with server settings

Use these tasks to configure and maintain server settings. Only the general server settings are covered here. Feature-specific server settings are covered in the sections that cover those features. For example, System Tree sorting server settings are covered in *Organizing Systems for Management*.

Tasks

- Specifying an email server
- Configuring the template and location for exported reports
- Determining which events are forwarded to the server
- Viewing and changing communication ports

Specifying an email server

Use this task to specify an email server that ePolicy Orchestrator usea to send email messages.

Task

For option definitions, click **?** on the page displaying the options.

1. Go to **Configuration | Server Settings**, then click **Email Server** in the **Settings** list.
2. Click **Edit**. The **Edit Email Server** page appears.
3. Type the SMTP server name and SMTP server port.
4. Select whether to authenticate to the email server, and provide credentials if **Authenticate** is selected.
5. Type the email address of the return address on messages sent from ePolicy Orchestrator.
6. Click **Save**, then select **Email Server**.
7. In the content area next to **Test email**, type a valid email address for receiving email messages, then click **Test** to validate the settings.

Configuring the template and location for exported reports

Use this task to define the appearance and storage location for tables and dashboards you export as documents. You can configure:

- Headers and footers, including a custom logo, name, page numbering, etc.
- Page size and orientation for printing.
- Directory where exported tables and dashboards are stored.

Task

For option definitions, click **?** on the page displaying the options.

1. Go to **Configuration | Server Settings,** then select **Printing and Exporting** in the **Settings** list.
2. Click **Edit**. The **Edit Printing and Exporting** page appears.
3. Next to **Headers and footers for exported documents**:
   a. Click **Edit Logo** to provide a custom image or text to use as the header.
   b. Select the desired metadata from the drop-down lists that you want displayed in the header and footer.
   c. Select a **Page size**.
   d. Select a **Page orientation**.
4. Type a new location or except the default location to save exported documents.
5. Click **Save**.

Determining which events are forwarded to the server

Use this task to determine which events are forwarded to the server. This selection impacts the bandwidth used in your environment, as well as the results of event-based queries.

Before you begin

You must be a global administrator to perform this task.

Task

For option definitions, click **?** on the page displaying the options.

1 Go to **Configuration | Server Settings**, select **Event Filtering**, then click **Edit** at the bottom of the page. The **Edit Event Filtering** page appears.

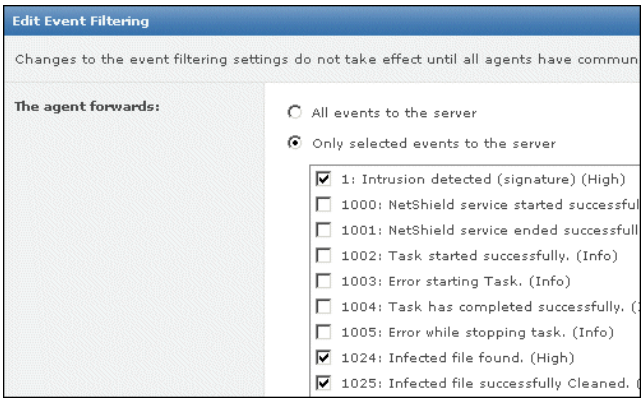
Edit Event Filtering
Changes to the event filtering settings do not take effect until all agents have commun
The agent forwards:
All events to the server
Only selected events to the server
1: Intrusion detected (signature) (High)
1000: NetShield service started successful
1001: NetShield service ended successfull
1002: Task started successfully. (Info)
1003: Error starting Task. (Info)
1004: Task has completed successfully. (
1005: Error while stopping task. (Info)
1024: Infected file found. (High)
1025: Infected file successfully Cleaned. (

Figure 3: Edit Event Filtering page

2 Select the events you want the agent to forward to the server, then click **Save**.

Changes to these settings take effect after all agents have communicated with the ePO server.

Viewing and changing communication ports

Use this task to view the ports ePolicy Orchestrator uses for communication with distributed components. These ports were originally configured during installation. After installation you can only change the two ports used for agent communication. If you need to change other ports, you must reinstall the server and reconfigure the ports in the installation wizard.

Task

For option definitions, click **?** on the page displaying the options.

1 Go to **Configuration | Server Settings**, select **Ports**, then click **Edit** at the bottom of the page. The **Edit Ports** page appears.

2 Change the agent-server communication or agent broadcast communication ports as necessary, then click **Save**.

NOTE: The agent-server communication port is used for agent-server communication; the agent broadcast port is used for SuperAgent wake-up calls.

Working with the Server Task Log

Use these tasks to view and maintain the Server Task Log.

Tasks

- Viewing the Server Task Log

Filtering the Server Task Log
Purging the Server Task Log

Viewing the Server Task Log

Use this task to review the status of server tasks and long-running actions.

The status of each server task appears in the **Status** column:

- **Completed** — Task completed successfully.
- **Failed** — Task was started but did not complete successfully.
- **In progress** — Task has started but not finished.
- **Waiting** — This message appears when the task is waiting for another task to finish.
- **Terminated** — Task was terminated before it finished.

Task

For option definitions, click **?** on the page displaying the options.

1 Go to **Reporting | Server Task Log**.

2 Click any entry in the log to view its details.

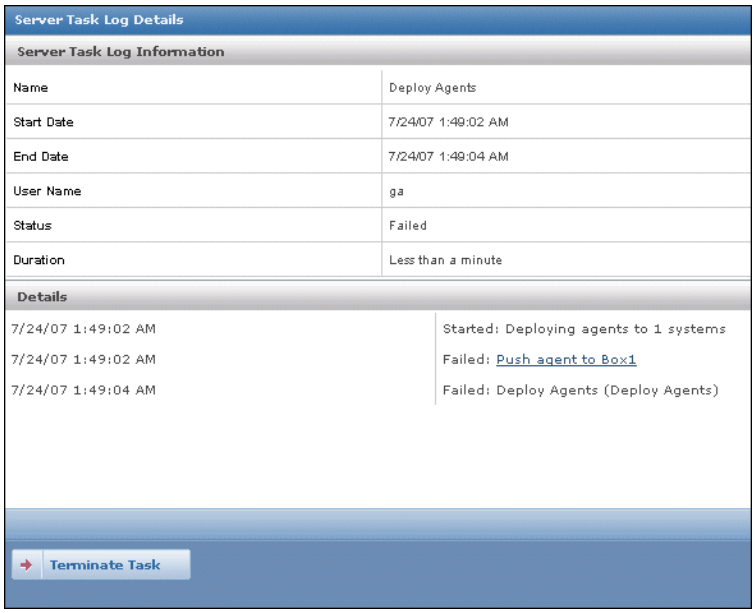

Figure 4: Server Task Log Details page

Filtering the Server Task Log

As the Server Task Log grows, you can filter it to show only the most recent activity. You can filter the log to show only entries from the last day, last seven days, last 30 days, or by Failed or In Progress task statuses.

Task

For option definitions, click **?** on the page displaying the options.

1 Go to **Reporting | Server Task Log**.

2 Select the desired filter from the **Filter** drop-down list.

Purging the Server Task Log

As the Server Task Log grows, you can purge items older than a user-configurable number of days, weeks, months, or years.

Task

For option definitions, click **?** on the page displaying the options.

1 Go to **Reporting | Server Task Log**, then click **Purge**.

2 In the **Action** panel, type a number of days, weeks, months, or years. All items of this age and older are deleted.

3 Click **OK**.

Working with the Audit Log

Use these tasks to view and purge the Audit Log. The Audit Log records actions taken by ePO users.

Tasks

- Viewing the Audit Log
- Purging the Audit Log
- Purging the Audit Log on a schedule

Viewing the Audit Log

Use this task to view a history of administrator actions. Available data depends on how often and by what age the Audit Log is purged.

Before you begin

You must have appropriate permissions to perform this task.

Task

For option definitions, click **?** on the page displaying the options.

1 Go to **Reporting | Audit Log**. The details of administrator actions are displayed in a table.

Audit Log

Start Time ▼	User Name	Action	Priority
7/24/07 7:29:56 PM PDT	admin	Delete Dashboard	Medium
7/24/07 7:29:42 PM PDT	admin	Delete Dashboard	Medium
7/24/07 7:29:35 PM PDT	admin	Delete Dashboard	Medium
7/24/07 7:29:28 PM PDT	admin	Delete Dashboard	Medium
7/24/07 7:18:01 PM PDT	admin	Login attempt	Low
7/24/07 10:37:10 AM PDT	admin	User Logout	Low

Figure 5: Audit Log page

2 Click any of the column titles to sort the table by that column (alphabetically).

3 From the **Filter** drop-down list, select an option to narrow the amount of visible data. You can remove all but the failed actions, or only show actions that occurred within a selected amount of time.

4 Click any entry to view its details.

Figure 6: Audit Log Entry Details page

Purging the Audit Log

Use this task to purge the Audit Log. You can only purge Audit Log records by age. when you purge the Audit Log, the records are deleted permanently.

Before you begin

You must have appropriate permissions to perform this task.

Task

For option definitions, click **?** on the page displaying the options.

1 Go to **Reporting | Audit Log**.

2 Click **Purge**.

3 In the **Action** panel, next to **Purge records older than**, type a number and select a time unit.

4 Click **OK**.

All records older than the specified time frame are purged.

Purging the Audit Log on a schedule

Use this task to purge the Audit Log with a scheduled server task.

Before you begin

You must have appropriate permissions to perform this task.

Task

For option definitions, click **?** on the page displaying the options.

1 Go to **Automation | Server Tasks**, then click **New Task**. The **Description** page of the **Server Task Builder** wizard appears.

2 Name and describe the task, then click **Next**. The **Actions** page appears.

3 Select **Purge Audit Log** from the drop-down list.
4 Select whether to purge by age or from a queries results. If you purge by query, you must pick a query that results in a table of Audit Log entries.
5 Click **Next**. The **Schedule** page appears.
6 Schedule the task as needed, then click **Next**. The **Summary** page appears.
7 Review the task's details, then click **Save**.

Working with the Event Log

Use these tasks to view and puge the Event Log

Tasks

- Viewing the Event Log
- Purging events
- Purging the Event Log on a schedule

Viewing the Event Log

Use this task to view the Event Log.

Before you begin

You must have appropriate permissions to perform this task.

Task

1 Go to **Reporting | Event Log**.
2 Click any of the column titles to sort the events. You can also select **Choose Columns** from the **Options** drop-down list to select different table columns that meet your needs.
3 Select events in the table, then click **Show Related Systems** to see the details of the systems that sent the selected events.

Purging events

Use this task to purge event records from the database. Purging event records deletes them permanently.

Before you begin

You must have appropriate permissions to perform this task.

Task

For option definitions, click **?** on the page displaying the options.

1 Go to **Reporting | Event Log**.
2 Click **Purge**.
3 In the **Actions** panel, next to **Purge records older than**, type a number and select a time unit.

4 Click **OK**.

Records older than the specified age are deleted permanently.

Purging the Event Log on a schedule

Use this task to purge the Event Log with a scheduled server task.

Before you begin

You must have appropriate permissions to perform this task.

Task

For option definitions, click **?** on the page displaying the options.

1 Go to **Automation | Server Tasks**, then click **New Task**. The **Description** page of the **Server Task Builder** wizard appears.

2 Name and describe the task, then click **Next**. The **Actions** page appears.

3 Select **Purge Event Log** from the drop-down list.

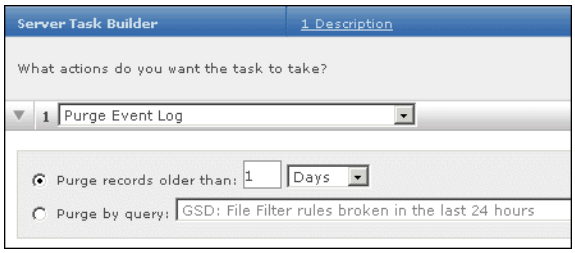

Figure 7: Purge Event Log server task action

4 Select whether to purge by age or from a queries results. If you purge by query, you must pick a query that results in a table of events.

5 Click **Next**. The **Schedule** page appears.

6 Schedule the task as needed, then click **Next**. The **Summary** page appears.

7 Review the task's details, then click **Save**.

Working with MyAvert Security Threats

Use these task to mark threat notifications as read or unread or delete them. Data is sorted by the date the threat was discovered. In addition, you can click the threat name to go to view information from the McAfee Avert website about each threat.

NOTE: Each user views a **MyAvert** page that is unique to their account. When one user deletes, or marks threat notifications as read or unread, these actions are not represented in the table when another user account logs on.

Tasks

- Configuring MyAvert update frequency and proxy settings
- Viewing threat notifications
- Deleting threat notifications

Configuring MyAvert update frequency and proxy settings

Use this task to configure proxy settings adn the update frequency for MyAvert Security Threats.

Task

1. Go to **Configuration | Server Settings**, select **MyAvert Security Threats**, then click **Edit**.
2. Choose how often you want the MyAvert threat notifications updated.
3. Then choose whether to use a proxy to access this service. If you select to use a proxy, provide the required details to use your proxy.

Viewing threat notifications

Use this task to view notification threats and mark threats as read or unread. You can filter threats by their importance, or whether they've been marked read, or unread.

Task

For option definitions, click **?** on the page displaying the options.

1. Go to **Reporting | MyAvert**.

Figure 8: MyAvert Security Threats page

2. If you want to narrow the viewable notifications, select an option from the **Filter** drop-down list.
3. If you want to mark notifications as read or unread, select the desired threats, then click **Mark Read** or **Mark Unread**, as needed. You may need to select **Read** or **Unread** from the **Filter** drop-down list to view the notifications you want to mark.

Deleting threat notifications

Use this task to delete threat notifications from the **MyAvert** page. You cannot delete any threat notifications for which protection is still pending.

Task

For option definitions, click **?** on the page displaying the options.

1. Go to **Reporting | MyAvert**.
2. Select threat notifications for which protection is available, then click **Delete**.

Exporting tables and charts to other formats

Use this task to export data for other purposes. You can export to HTML and PDF finals for viewing formats, or to CSV or XML files for using and transforming the data in other applications.

Task

For option definitions, click **?** on the page displaying the options.

1 From the page displaying the data (tables or charts), select **Export Table** or **Export Data** from the **Options** menu. The **Export** page appears.

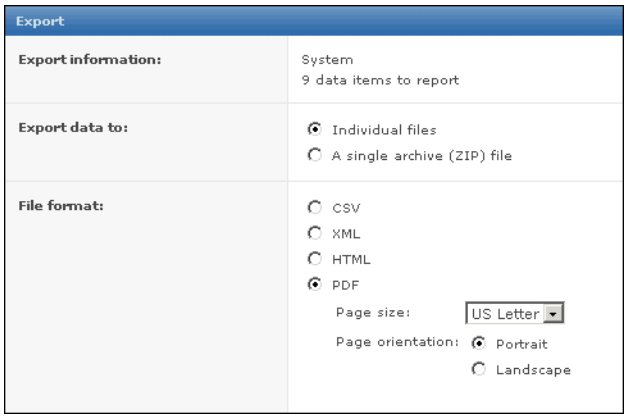

Figure 9: Export page

2 Select whether the data files are exported individually or in a single archive (ZIP) file.

3 Select the format of the exported file. If exporting to a PDF file, select the page size and orientation.

4 Select whether the files are emailed as attachments to selected recipients, or whether they are saved to a location on the server to which a link is provided. You can open or save the file to another location by right-clicking it.

NOTE: When typing multiple email addresses for recipients, you must separate entries with a comma or semi-colon.

5 Click **Export**.

The files are created and either emailed as attachments to the recipients, or you are taken to a page where you can access the files from links.

Allowed Cron syntax when scheduling a server task

Cron syntax is made up of 6 or 7 fields, separated by a space. Accepted Cron syntax, by field in descending order, is detailed below in the table. Most Cron syntax is acceptable, however there are a few cases that are not supported. For example, you cannot specify both the Day of Week and Day of Month values.

Field Name	Allowed Values	Allowed Special Characters
Seconds	0 - 59	, - * /
Minutes	0 - 59	, - * /

Field Name	Allowed Values	Allowed Special Characters
Hours	0 - 23	, - * /
Day of Month	1 - 31	, - * ? / L W C
Month	1 - 12, or JAN - DEC	, - * /
Day of Week	1 -7, or SUN - SAT	, - * ? / L C #
Year (optional)	Empty, or 1970 - 2099	, - * /

Notes on allowed special characters

- Commas (,) are allowed to specify additional values. For example, "5,10,30" or "MON,WED,FRI".
- Asterisks (*) are used for "every." For example, "*" in the minutes field is "every minute".
- Question marks (?) are allowed to specify no specific value in the Day of Week or Day of Month fields.

  NOTE: The question mark must be used in one of these fields, but cannot be used in both.

- Forward slashes (/) identify increments. For example, "5/15" in the minutes field means the task runs at minutes 5, 20, 35 and 50.
- The letter "L" means "last" in the Day of Week or Day of Month fields. For example, "0 15 10 ? * 6L" means the last Friday of every month at 10:15 am.
- The letter "W" means "weekday". So, if you created a Day of Month as "15W", this means the weekday closest to the 15th of the month. Also, you can specify "LW", which would mean the last weekday of the month.
- The pound character "#" identifies the "Nth" day of the month. For example, using "6#3" in the Day of Week field is the third Friday of every month, "2#1" is the first Monday, and "4#5" is the fifth Wednesday.

  NOTE: If the month does not have fifth Wednesday, the task does not run.

Organizing Systems for Management

ePolicy Orchestrator 4.0.2 provides some new features and improvements to existing features to organize and manage your systems.

- The Directory has been replaced by the System Tree — The System Tree allows for easy management of policies and tasks, and organization of systems and groups.
- Tags — This new feature allows you to create labels that can be applied to systems manually or automatically, based on criteria assigned to the tag. You can sort systems into groups based on tags (like IP address sorting), or use tags for criteria in queries.
- NT Domain and Active Directory synchronization — This feature now allows for:
  - True synchronization of the Active Directory structure.
  - Control of potential duplicate system entries in the System Tree.
  - Control of systems in the System Tree when they are deleted from the the domain or container.
- Sorting systems into groups automatically — You can now use tags as sorting criteria in addition to the previous functionalities of IP address sorting. Each type of sorting criteria can be used alone or in combination.

The System Tree contains all of the systems managed by ePolicy Orchestrator; it is the the primary interface for managing policies and tasks on these systems. You can organize systems into logical groups (for example, functional department or geographic location) and sort them by IP address or tags. You can manage policies (product configuration settings) and schedule tasks (for example, updating virus definition files) for systems at any level of the System Tree.

Before configuring the software to deploy or manage the security software in your environment, you must plan how to best organize systems for management and select the methods to bring in and keep systems in the System Tree.

TIP: Many factors can influence how you should create and organize your System Tree. McAfee recommends taking time to review this entire guide before you begin creating your System Tree.

Are you setting up the System Tree for the first time?

When setting up the System Tree for the first time:

1. Reviewing the conceptual topics in this section to so you can use it with other features to organize your systems efficently.
2. Evaluate the methods of populating it with your systems, and keeping it up-to-date. For example, through Active Directory synchronization, or criteria-based sorting.
3. Create and populate the System Tree.

Contents

- The System Tree
- Considerations when planning your System Tree
- Tags and how they work
- Active Directory and NT domain synchronization
- Criteria-based sorting
- How a system is first placed in the System Tree
- Working with tags
- Creating and populating groups
- Moving systems manually within the System Tree

The System Tree

The System Tree organizes managed systems in units for monitoring, assigning policies, scheduling tasks, and taking actions.

Groups

The System Tree is a hierarchical structure that allows you to group your systems within units called *groups*.

Groups have these characteristics:

- Groups can be created by global administrators or users with the appropriate permissions.
- A group can include both systems and other groups.
- Groups are administered by a global administrator or a user with appropriate permissions.

Grouping systems with similar properties or requirements into these units allows you to manage policies for systems in one place, rather than setting policies for each system individually.

As part of the planning process, consider the best way to organize systems into groups prior to building the System Tree.

Lost&Found group

The System Tree root (My Organization) includes a Lost&Found group. Depending on the methods for creating and maintaining the System Tree, the server uses different characteristics to determine where to place systems. The Lost&Found group stores systems whose locations could not be determined.

The Lost&Found group has the following characteristics:

- It can't be deleted.
- It can't be renamed.
- Its sorting criteria can't be changed (although you can provide sorting criteria for the subgroups you create within it.)
- It always appears last in the list and is not alphabetized among its peers.
- All users with view permissions to the System Tree can see systems in Lost&Found.

- When a system is sorted into Lost&Found, it is placed in a subgroup named for the system's domain. If no such group exists, one is created.

NOTE: If you delete systems from the System Tree, you also need to remove their agents. Otherwise, these systems continue to appear in the Lost&Found group because the agent continues to communicate to the server.

Inheritance

Inheritance is an important property that simplifies policyand task administration. Because of inheritance, child groups in the System Tree hierarchy inherit policies set at their parent groups. For example:

- Policies set at the My Organization level of the System Tree are inherited by groups below it.
- Group policies are inherited by subgroups or individual systems within that group.

Inheritance is enabled by default for all groups and individual systems that you add to the System Tree. This allows you to set policies and schedule client tasks in fewer places.

However, inheritance can be broken by applying a new policy at any location of the System Tree (provided a user has appropriate permissions) to allow for customization. You can lock policy assignments to preserve inheritance.

Considerations when planning your System Tree

An efficient and well-organized System Tree can simplify maintenance. Many administrative, network, and political realities of each environment can affect how your System Tree is structured. Plan the organization of the System Tree before you build and populate it. Especially for a large network, you want to build the System Tree only once.

Because every network is different and requires different policies — and possibly different management — McAfee recommends planning your System Tree before implementing the software.

Regardless of the methods you choose to create and populate the System Tree, consider your environment while planning the System Tree.

Administrator access

When planning your System Tree organization, consider the access requirements of those who must manage the systems.

For example, you may have very decentralized network administration in your organization, where different administrators have responsibilities over different parts of the network. For security reasons, you may not have a global administrator account that can access every part of your network. In this scenario, you may not be able to set policies and deploy agents using a single global administrator account. Instead, you may need to organize the System Tree into groups based on these divisions and create accounts and permission sets.

Questions to consider include:

- Who is responsible for managing which systems?
- Who requires access to view information about the systems?
- Who should not have access to the systems and the information about them?

These questions impact both the System Tree organization, and the permission sets you create and apply to user accounts.

Environmental borders and their impact on system organization

How you organize the systems for management depends on the borders that exist in your network. These borders influence the organization of the System Tree differently than the organization of your network topology.

McAfee recommends evaluating these borders in your network and organization, and whether they must be considered when defining the organization of your System Tree.

Topological borders

Your network is already defined by NT domains or Active Directory containers. The better organized your network environment, the easier it is to create and maintain the System Tree with the synchronization features.

Geographic borders

Managing security is a constant balance between protection and performance. Organize your System Tree to make the best use of limited network bandwidth. Consider how the server connects to all parts of your network, especially remote locations that are often connected by slower WAN or VPN connections, instead of faster LAN connections. You may want to configure updating and agent-server communication policies differently for remote sites to minimize network traffic over slower connections.

Grouping systems first by geography provides several advantages for configuring policies:

- You can configure update policies for the group so that all systems update from one or more distributed software repositories located nearby.
- You can schedule client tasks to run at times better suited to the site's location.

Political borders

Many large networks are divided by individuals or groups responsible for managing different portions of the network. Sometimes these borders do not coincide with topological or geographic borders. Who accesses and manages the segments of the System Tree affects how you structure it.

Functional borders

Some networks are divided by the roles of those using the network; for example, Sales and Engineering. Even if the network is not divided by functional borders, you may need to organize segments of the System Tree by functionality if different groups require different policies.

A business group may run specific software that requires special security policies. For example, arranging your email exchange servers into a group and setting specific exclusions for VirusScan Enterprise on-access scanning.

Subnets and IP address ranges

In many cases, organizational units of a network use specific subnets or IP ranges, so you can create a group for a geographic location and set IP filters for it. Also, if your network isn't spread out geographically, you can use network location, such as IP address, as the primary grouping criterion.

If possible, consider using sorting criteria based on IP address information to automate System Tree creation and maintenance. Set IP subnet masks or IP address range criteria for applicable groups within the System Tree. These filters automatically populate locations with the appropriate systems.

Tags and systems with similar characteristics

You can use tags for automated sorting into groups. Tags identify systems with similar characteristics. If you can organize your groups by characteristics, you can create and assign tags based on that criteria, then use these tags as group sorting criteria to ensure systems are automatically placed within the appropriate groups.

If possible, consider using tag-based sorting criteria to automatically populate groups with the appropriate systems.

Operating systems and software

Consider grouping systems with similar operating systems to manage operating system-specific products and policies more easily. If you have some older systems running Windows 95 or Windows 98. You can create a group for such legacy systems together to deploy and manage security products on these systems separately. Additionally, by giving these systems a corresponding tag, you can automatically sort them into a group.

Tags and how they work

Tags are a new feature of ePolicy Orchestrator 4.0.2. Tags are like labels that you can apply to one or more systems, automatically (based on criteria) or manually. Once tags are applied, you can use them organize systems in the System Tree or run queries that result in an actionable list of systems. Therefore, with tags as organizational criteria, you can apply policies, assign tasks, and take a number of actions on systems with the same tags.

Traits of tags

With tags, you can:

- Apply one or more tags to one or more systems.
- Apply tags manually.
- Apply tags automatically, based on user-defined criteria, when the agent communicates with the server.
- Exclude systems from tag application.
- Run queries to group systems with certain tags, then take direct action on the resulting list of systems.
- Base System Tree sorting criteria on tags to group systems into desired System Tree groups automatically.

Who can use tags

Users with appropriate permissions can:

- Create and edit tags and tag criteria.

- Apply and remove existing tags to systems in the groups to which they have access.
- Exclude systems from receiving specific tags.
- Use queries to view and take actions on systems with certain tags.
- Use scheduled queries with chained tag actions to maintain tags on specific systems within the parts of the System Tree they have access.
- Configure sorting criteria based on tags to ensure systems stay in the appropriate groups of the System Tree.

Types of tags

There are two types of tags:

- Tags without criteria. These tags can be applied only to selected systems in the System Tree (manually) and systems listed in the results of a query.
- Criteria-based tags. These tags are applied to all non-excluded systems at each agent-server communication. Such tags use criteria based on any properties sent by agent. They can also be applied to non-excluded systems on demand.

Active Directory and NT domain synchronization

ePolicy Orchestrator 4.0.2 offers improved integration with both Active Directory and NT domains as a source for systems, and even (in the case of Active Directory) as a source for the structure of the System Tree.

Active Directory synchronization

If your network runs Active Directory, you can use Active Directory synchronization to create, populate, and maintain part or all of the System Tree with Active Directory synchronization settings. Once defined, the System Tree is updated with any new systems (and subcontainers) in your Active Directory.

Active Directory integration is enhanced with the release of ePolicy Orchestrator 4.0.2. In addition to previous functionality, you can now:

- Synchronize with your Active Directory structure, by importing systems and the Active Directory subcontainers (as System Tree groups) and keeping them up-to-date with Active Directory. At each synchronization, both systems and the structure are updated in the System Tree to reflect the systems and structure of Active Directory.
- Import systems as a flat list from the Active Directory container (and its subcontainers) into the synchronized group.
- Control what to do with potential duplicate systems.
- Use the system description, which is imported from Active Directory with the systems.

In previous versions of ePolicy Orchestrator, there were the two tasks: Active Directory Import and Active Directory Discovery. Now, use this process to integrate the System Tree with your Active Directory systems structure:

1 Configure the synchronization settings on each group that is a mapping point in the System Tree. At the same location, you can configure whether to:

2 • Deploy agents to discovered systems.

- Delete systems from the System Tree when they are deleted from Active Directory.
- Allow or disallow duplicate entries of systems that already exist elsewhere in the System Tree.

3 Use the Synchronize Now action to import Active Directory systems (and possibly structure) into the System Tree according to the synchronization settings.

4 Use an NT Domain/Active Directory Synchronization server task to regularly synchronize the systems (and possibly the Active Directory structure) with the System Tree according to the synchronization settings.

Types of Active Directory synchronization

There are two types of Active Directory synchronization (systems only and systems and structure). Which one you use depends on the level of integration you want with Active Directory.

With each type, you control the synchronization by selecting whether to:

- Deploy agents automatically to systems new to ePolicy Orchestrator. You may not want to set this on the initial synchronization if you are importing a large number of systems and have limited bandwidth. The agent installation package is about 3.62 MB in size. However, you may want to deploy agents automatically to any new systems that are discovered in Active Directory during subsequent synchronizations.
- Delete systems from ePolicy Orchestrator (and remove their agents) when they are deleted from Active Directory.
- Prevent adding systems to the group if they exist elsewhere in the System Tree. this ensures no duplicate systems if you manually move or sort the system to another location.
- Exclude certain Active Directory containers from the synchronization. These containers and their systems are ignored during synchronization.

Systems and structure

When using this synchronization type, changes in the Active Directory structure are carried over into your System Tree structure at the next synchronization. When systems or containers are added, moved, or removed in Active Directory, they are added, moved, or removed in the corresponding locations of the System Tree.

When to use this synchronization type

Use this to ensure the System Tree (or parts of it) look exactly like your Active Directory structure.

If the organization of Active Directory meets your security management needs and you want the System Tree to continue to look like the mapped Active Directory structure, use this synchronization type with subsequent synchronizations.

Systems only

Use this synchronization type to import systems from an Active Directory container, including those in non-excluded subcontainers, as a flat list to a mapped System Tree group. You can then move these to the desired locations in the System Tree by assigning sorting criteria to groups.

If you choose this synchronization type, be sure to select not to add systems again if they exist elsewhere in the System Tree. This prevents duplicate entries for systems in the System Tree.

When to use this synchronization type

Use this synchronization type when you use Active Directory as a regular source of systems for ePolicy Orchestrator, but the organizational needs for security management do not coincide with the organization of containers and systems in Active Directory.

NT domain synchronization

Use your NT domains as a source for populating your System Tree. When you synchronize a group to an NT domain, all systems from the domain are put in the group as a flat list. You can manage those systems in the single group, or you can create subgroups for more granular organizational needs. Use a method, like automatic sorting to populate these subgroups automatically.

If you move systems to other groups or subgroups of the System Tree, be sure to select to not add the systems when they already exist elsewhere in the System Tree.

Unlike Active Directory synchronization, only the system names are synchronized with NT domain synchronization — the system description is not synchronized.

Criteria-based sorting

As in past releases of ePolicy Orchestrator, you can use IP address information to automatically sort managed systems into specific groups. You can also create sorting criteria based on tags, which are like labels assigned to systems. You can use either type of criteria or both to ensure systems are where you want them in the System Tree.

Systems only need to match one criterion of a group's sorting criteria to be placed in the group.

After creating groups and setting your sorting criteria, take a Test Sort action to confirm the criteria and sorting order achieve the desired results.

Once you have added sorting criteria to your groups, you can run the Sort Now action. The action moves selected systems to the appropriate group automatically. Systems that do not match the sorting criteria of any group are moved to Lost&Found.

New systems that call into the server for the first time are added automatically to the correct group. However, if you define sorting criteria after the initial agent-server communication, you must run the Sort Now action on those systems to move them immediately to the appropriate group, or wait until the next agent-server communication.

Sorting status of systems

On any system or collection of systems, you can enable or disable System Tree sorting. If you disable System Tree sorting on a system, it is excluded from sorting actions.

System Tree sorting settings on the ePO server

For sorting to take place, sorting must be enabled on the server and on the systems. By default, sorting at each agent-server communication is enabled.

Test sorting systems

Use this feature to view where systems would be placed during a sort action. The **Test Sort** page displays the systems and the paths to the location where they would be sorted. Although this page does not display the sorting status of systems, if you select systems on the page

(even ones with sorting disabled) clicking **Move Systems** places those systems in the location identified.

How settings affect sorting

You can choose three server settings that determine whether and when systems are sorted. Also, you can choose whether any system can be sorted by enabling or disabling System Tree sorting on selected systems in the System Tree.

Server settings

The server has three settings:

- **Disable System Tree sorting** — If criteria-based sorting does not meet your security management needs and you want to use other System Tree features (like Active Directory synchronization) to organize your systems, select this setting to prevent other ePO users from mistakenly configuring sorting criteria on groups and moving systems to undesirable locations.
- **Sort systems on each agent-server communication** — Systems are sorted again at each agent-server communication. When you change sorting criteria on groups, systems move to the new group at their next agent-server communication.
- **Sort systems once** — Systems are sorted at the next agent-server communication and marked to never be sorted again at agent-server communication as long as this setting is selected. However, selecting such a system and clicking **Sort Now** does sort the system.

System settings

You can disable or enable System Tree sorting on any system. If System Tree sorting is disabled on a system, that system will not be sorted regardless of how the sorting action is taken. If System Tree sorting is enabled on a system, that system is sorted always for the manual Sort Now action, and may be sorted at agent-server communication, depending on the System Tree sorting server settings.

IP address sorting criteria

In many networks, subnets and IP address information reflect organizational distinctions, such as geographical location or job function. If IP address organization coincides with your needs, consider using this information to create and maintain parts or all of your System Tree structure by setting IP address sorting criteria for such groups. This functionality has changed in this version of ePolicy Orchestrator, which now allows for setting of IP sorting criteria randomly through the tree — you no longer need to ensure that the child group's IP address sorting criteria is a subset of the parent's (as long as the parent has no assigned criteria). Once configured, you can sort systems at agent-server communication, or only when a sort action is manually initiated.

Please know that IP address sorting criteria should not overlap between different groups. Each IP range or subnet mask in a group's sorting criteria should cover a unique set of IP addresses. If criteria does overlap, which group those systems end up in depends on the order of the subgroups on the **Groups** tab.

Tag-based sorting criteria

In addition to using IP address information to sort systems into the appropriate group, you can define sorting criteria based on the tags assigned to systems.

Tag-based criteria can be used with IP address-based criteria for sorting.

Group order and sorting

To provide additional flexibility with System Tree management, you can configure the order of a group's subgroups, and therefore the order by which they are considered for a system's placement during sorting. When multiple subgroups have matching criteria, changing this order can change where a system ends up in the System Tree.

Additionally, if you are using catch-all groups, they must be the last subgroup in the list.

Catch-all groups

Catch-all groups are groups whose sorting criteria is set to **All others** on the **Sorting Criteria** page of the group. Only subgroups at the last position of the sort order can be catch-all groups. These groups receive all systems that sorted into the parent group, but did not sort into any of the catch-all's peers.

How a system is first placed in the System Tree

When the agent communicates with the server for the first time, the server uses an algorithm to place the system in the System Tree. When it cannot find any location for a system, it puts the system in the Lost&Found group.

At the first agent-server communication

On each agent-server communication, the server attempts to locate the system in the System Tree by agent GUID (only systems whose agents have already called into the server for the first time have an agent GUID in the database). If a matching system is found, it is left in it's existing location.

If a matching system is not found, the server uses an algorithm to sort the systems into the appropriate groups. Systems can be sorted into any criteria-based group in the System Tree, no matter how deep it is in the structure, as long as each parent group in the path does not have non-matching criteria. Parent groups of a criteria-based subgroup must either have no criteria or matching criteria.

Remember, the order subgroups are placed the **Group** tab, determines the order subgroups are considered by the server when it searches for a group with matching criteria.

1. The server searches for a system without an agent GUID (its agent has never called in before) with a matching name in a group with the same name as the domain. If found, the system is placed in that group. This can happen after the first Active Directory or NT domain synchronization, or when you have manually added systems to the System Tree.
2. If a matching system is still not found, the server searches for a group of the same name as the domain from which the system originates. If such a group is not found, one is created under the Lost&Found group, and the system placed there.
3. Properties are updated for the system.

4 The server applies all criteria-based tags to the system if the server is configured to run sorting criteria at each agent-server communication.

5 What happens next depends on whether System Tree sorting is enabled on both the server and the system.

- If System Tree sorting is disabled on either the server or the system, the system is left where it is.
- If System Tree sorting is enabled on the server and system, the system is moved based on the sorting criteria in the System Tree groups.

  NOTE: Systems that are added by Active Directory or NT Domain synchronization have System Tree sorting disabled by default. Therefore, they are not sorted on the first agent-server communication

6 The server considers the sorting criteria of all top-level groups according to the sorting order on the My Organization group's **Group** tab. The system is placed in the first group with matching criteria or a catch-all group it considers.

a Once sorted into a group, each of its subgroups are considered for matching criteria according to their sorting order on the Group tab.

b This continues until there is no subgroup with matching criteria for the system, and is placed in the last group found with matching criteria.

7 If such a top-level group is not found, then the subgroups of top-level groups (without sorting criteria) are considered according to their sorting.

8 If such a second-level criteria-based group is not found, then the criteria-based third-level groups of the second-level unrestricted groups considered.

NOTE: Subgroups of groups with unmatching criteria are not considered, a group must have matching criteria or have no criteria in order for its subgroups to be considered for a system.

9 This continues down through the System Tree until a system is sorted into a group.

NOTE: If the server System Tree sorting setting is configured to sort only on the first agent-server communication, a flag is set on the system and it can never be sorted again at agent-server communication unless the server setting is changed to enable sorting on every agent-server communication.

10 If the server cannot sort the system into any group, it is placed in the Lost&Found group within a subgroup named after its domain.

Working with tags

Use these tasks to create and apply tags to systems.

Tasks

- Creating tags with the Tag Builder
- Excluding systems from automatic tagging
- Applying tags to selected systems
- Applying criteria-based tags automatically to all matching

Creating tags with the Tag Builder

Use this task to create a tag with the **Tag Builder** wizard. Tags can use criteria that's evaluated against every system:

- Automatically at agent-server communication.
- When the Run Tag Criteria action is taken.
- Manually on selected systems, regardless of criteria, with the Apply Tag action.

Tags without criteria can only be applied manually to selected systems.

Task

For option definitions, click **?** on the page displaying the options.

1. Go to **Systems | System Tree | Tag Catalog**, then click **New Tag**. The **Description** page of the **Tag Builder** wizard appears.
2. Type a name and meaningful description, then click **Next**. The **Criteria** page appears.
3. Select and configure the desired criteria, then click **Next**. The **Evaluation** page appears.

   NOTE: To apply the tag automatically, you must configure criteria for the tag.

4. Select whether systems are evaluated against the tag's criteria only when the Run Tag Criteria action is taken, or also at each agent-server communication, then click **Next**. The **Preview** page appears.

   NOTE: These options are unavailable if criteria was not configured. When systems are evaluated against a tag's criteria, the tag is applied to systems that match the criteria and have not been excluded from the tag.

5. Verify the information on this page, then click **Save**.

   NOTE: If the tag has criteria, this page displays the number of systems that will receive this tag when evaluated against its criteria.

The tag is added to the list of tags on the **Tag Catalog** page.

Excluding systems from automatic tagging

Use this task to exclude systems from having specifc tags applied. Alternatively, you can use a query to collect systems, then exclude the desired tags from those systems from the query results.

Task

For option definitions, click **?** on the page displaying the options.

1. Go to **Systems | System Tree**, then select the group that contains the systems.
2. Select the desired systems, then click **Exclude Tag** at the bottom of the page.

   NOTE: If you don't see this button, click **More Actions**.

3. In the **Action** panel, select the desired tag to exclude from the selected systems from the drop-down list, then click **OK**.
4. Verify the systems have been excluded from the tag:

   a Go to **Systems | Tag Catalog**, then select the desired tag in the list of tags.

b Next to **Systems with tag** in the details pane, click the link for the number of systems excluded from automatic tagging. The **Systems Excluded from the Tag** page appears.

c Verify the desired systems are in the list.

Applying tags to selected systems

Use this task to apply a tag manually to selected systems in the System Tree.

Task

For option definitions, click **?** on the page displaying the options.

1 Go to **Systems | System Tree**, then select the group that contains the desired system.

2 Select the desired systems, then click **Apply Tag** at the bottom of the page.

NOTE: If you don't see this button, click **More Actions**.

3 In the **Action** panel, select the desired tag from the drop-down list to apply to the selected systems, then click **OK**.

4 Verify the tags have been applied:

a Go to **Systems | Tag Catalog**, then select the desired tag in the list of tags.

b Next to **Systems with tag** in the details pane, click the link for the number of systems tagged manually. The **Systems with Tag Applied Manually** page appears.

c Verify the desired systems are in the list.

Applying criteria-based tags automatically to all matching

Use these tasks to apply criteria-based tags automatically to all systems that match its criteria.

Tasks

- Applying criteria-based tags to all matching systems
- Applying criteria-based tags on a schedule

Applying criteria-based tags to all matching systems

Use this task to apply a criteria-based tag to all systems that match the criteria, except for those that have been excluded from the tag.

Task

For option definitions, click **?** on the page displaying the options.

1 Go to **Systems | Tag Catalog**, then select the desired tag from the **Tags** list.

2 Click **Run Tag Criteria**.

3 In the **Action** panel, select whether to reset manually tagged and excluded systems.

NOTE: This removes the tag from systems that don't match the criteria and applies the tag to systems which match criteria but were excluded from receiving the tag.

4 Click **OK**.

5 Verify the systems have the tag applied:

a Go to **Systems | Tag Catalog**, then select the desired tag in the list of tags.

b Next to **Systems with tag** in the details pane, click the link for the number of systems with tag applied by criteria. The **Systems with Tag Applied by Criteria** page appears.

c Verify the desired systems are in the list.

The tag is applied to all systems that match its criteria.

Applying criteria-based tags on a schedule

Use this task to schedule a regular task that applies a tag to all systems that match its criteria.

Task

For option definitions, click **?** on the page displaying the options.

1 Go to **Automation | Server Tasks**, then click **New Task**. The **Server Task Builder** page appears.

2 Name and describe the task and select whether the task is enabled once it is created, then click **Next**. The **Actions** page appears.

3 Select **Run Tag Criteria** from the drop-down list, then select the desired tag from the **Tag** drop-down list.

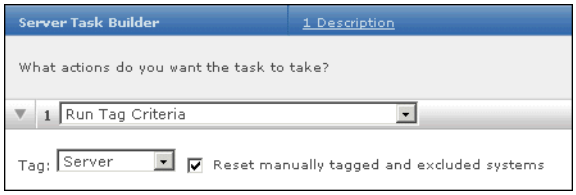

Figure 10: Run Tag Criteria server task action

4 Select whether to reset manually tagged and excluded systems.

NOTE: This removes the tag on systems that don't match the criteria and applies the tag to systems that match criteria but were excluded from receiving the tag.

5 Click **Next**. The **Schedule** page appears.

6 Schedule the task as desired, then click **Next**. The **Summary** page appears.

7 Review the task settings, then click **Save**.

The server task is added to the list on the **Server Tasks** page. If you selected to enable the task in the **Server Task Builder** wizard, it runs at the next scheduled time.

Creating and populating groups

Use these tasks to create and populate groups. You can populate groups with systems, either by typing NetBIOS names for individual systems or by importing systems directly from your network.

There is no single way to organize a System Tree, and because every network is different, your System Tree organization can be as unique as your network layout. Although you won't use each method offered, you can use more than one.

For example, if you use Active Directory in your network, consider importing your Active Directory containers rather than your NT domains. If your Active Directory or NT domain organization

does not make sense for security management, you can create your System Tree in a text file and import it into your System Tree. If you have a smaller network, you can create your System Tree by hand and import each system manually.

Best practices

While you won't use all of the System Tree creation methods, you also probably won't use just one. In many cases, the combination of methods you choose balances ease of creation with the need for additional structure to make policy management efficient.

For example, you might create the System Tree in two phases. First, you can create 90% of the System Tree structure by importing whole NT domains or Active Directory containers into groups. Then, you can manually create subgroups to classify systems together that may have similar anti-virus or security policy requirements. In this scenario, you could use tags, and tag-based sorting criteria on these subgroups to ensure they end up in the desired groups automatically.

If you want all or part of your System Tree to mirror the Active Directory structure, you can import and regularly synchronize the System Tree to Active Directory.

If one NT domain is very large or spans several geographic areas, you can create subgroups and point the systems in each to a separate distributed repository for efficient updating. Or, you can create smaller functional groupings, such as for different operating system types or business functions, to manage unique policies. In this scenario, you could also use tags and tag-based sorting criteria to ensure the systems stay in the group.

If your organization's IP address information coincides with your security management needs, consider assigning IP address sorting criteria to these groups before agent distribution, to ensure that when agents check into the server for the first time, the systems are automatically placed in the correct location. If you are implementing tags in your environment, you can also use tags as sorting criteria for groups, or even a combination of IP address and tag sorting criteria.

Although you can create a detailed System Tree with many levels of groups. McAfee recommends that you create only as much structure as is useful. In large networks, it is not uncommon to have hundreds or thousands of systems in the same container. Assigning policies in fewer places is easier than having to maintain an elaborate System Tree.

Although you can add all systems into one group in the System Tree, such a flat list makes setting different policies for different systems very difficult, especially for large networks.

Tasks

- Creating groups manually
- Adding systems manually to an existing group
- Importing systems from a text file
- Sorting systems into criteria-based groups
- Importing Active Directory containers
- Importing NT domains to an existing group
- Synchronizing the System Tree on a schedule
- Updating the synchronized group with an NT domain manually

Creating groups manually

Use this task to create groups manually. You can populate these groups with systems by typing NetBIOS names for individual systems or by importing systems directly from your network.

Task

For option definitions, click **?** on the page displaying the options.

1 Go to **Systems | System Tree | Group**, then select the desired group in the System Tree, under which to create another group.

2 Click **New Subgroup** at the bottom of the page. The **New Subgroup** dialog box appears.

3 Type the desired name then click **OK**. The new group appears in the System Tree.

4 Repeat as necessary until you are ready to populate the groups with the desired systems. Add systems to the System Tree and ensure they get to the desired groups by:

- Typing system names manually.
- Importing them from NT domains or Active Directory containers. You can regularly synchronize a domain or a container to a group for ease of maintenance.
- Setting up IP address-based or tag-based sorting criteria on the groups. When agents check in from systems with matching IP address information or matching tags, they are automatically placed in the appropriate group.

Adding systems manually to an existing group

Use this task to import systems from your Network Neighborhood to groups. You can also import a network domain or Active Directory container.

Task

For option definitions, click **?** on the page displaying the options.

1 Go to **Systems | System Tree**, then click **New Systems**. The **New Systems** page appears.

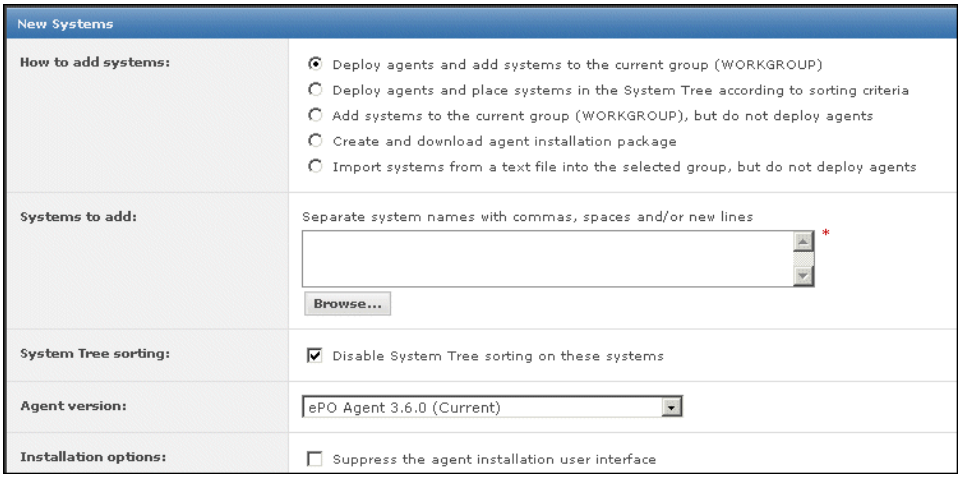
New Systems
How to add systems:
Deploy agents and add systems to the current group (WORKGROUP)
Deploy agents and place systems in the System Tree according to sorting criteria
Add systems to the current group (WORKGROUP), but do not deploy agents
Create and download agent installation package
Import systems from a text file into the selected group, but do not deploy agents
Systems to add:
Separate system names with commas, spaces and/or new lines
Browse...
System Tree sorting:
Disable System Tree sorting on these systems
Agent version:
ePO Agent 3.6.0 (Current)
Installation options:
Suppress the agent installation user interface

Figure 11: New Systems page

2 Select whether to deploy the agent to the new systems, and whether the systems are added to the selected group or to a group according to sorting criteria.

3 Next to **Systems to add**, type the NetBIOS name for each system in the text box, separated by commas, spaces, or line breaks. Alternatively, click **Browse** to select the systems.

4 If you selected **Deploy agents and add systems to the current group**, you can enable automatic System Tree sorting. Do this to apply the sorting criteria to these systems.

5 If you selected to deploy agents to the new systems:

a Select the agent version to deploy.

b Select whether to suppress the agent installation user interface on the system. Select this if you do not want the end-user to see the installation interface.

c Configure the agent installation path or accept the default.

d Type valid credentials to install the agent.

6 Click **OK**.

Importing systems from a text file

Use these tasks to create a text file of systems and groups to import into the System Tree.

Tasks

- Creating a text file of groups and systems
- Importing systems and groups from a text file

Creating a text file of groups and systems

Use this task to create a text file of the NetBIOS names for your network systems that you want to import into a group. You can import a flat list of systems, or organize the systems into groups, then add the specified systems to them. You can create the text file by hand. In large networks, use other network administration tools to generate a text file list of systems on your network.

Define the groups and their systems by typing the group and system names in a text file. Then import that information into ePolicy Orchestrator. You must have network utilities, such as the NETDOM.EXE utility available with the Microsoft Windows Resource Kit, to generate complete text files containing complete lists of the systems on your network. Once you have the text file, edit it manually to create groups of systems, and import the entire structure into the System Tree.

Regardless of how you generate the text file, you must use the correct syntax before importing it.

Task

For option definitions, click **?** on the page displaying the options.

1 List each system separately on its own line. To organize systems into groups, type the group name followed by a backslash (\), then list the systems belonging to that group beneath it, each on a separate line.

```
GroupA\system1
GroupA\system2
GroupA\system3
GroupA\system4
```

2 Verify the names of groups and systems, and the syntax of the text file, then save the text file to a temporary folder on your server.

Importing systems and groups from a text file

Use this task to import systems or groups of systems into the System Tree from a text file you have created and saved.

Task

For option definitions, click **?** on the page displaying the options.

1 Go to **Systems | System Tree**, then click **New Systems**. The **New Systems** page appears.

2 Select **Import systems from a text file into the selected group, but do not deploy agents**.

3 Click **Browse**, then select the text file.

4 Select what to do with systems that already exist elsewhere in the System tree.

5 Click **OK**.

The systems are imported to the selected group in the System Tree. If your text file organized the systems into groups, the server creates the groups and imports the systems.

Sorting systems into criteria-based groups

Use these tasks to configure and implement sorting to group systems. For systems to sort into groups, sorting must be enabled on the server and the desired systems, and sorting criteria and the sorting order of groups must be configured.

Tasks

- Adding sorting criteria to groups
- Enabling System Tree sorting on the server
- Enabling and disabling System Tree Sorting on Systems
- Sorting systems manually

Adding sorting criteria to groups

Use this task to configure sorting criteria for a group. Sorting criteria can be based on IP address information or tags.

Task

For option definitions, click **?** on the page displaying the options.

1 Go to **Systems | System Tree | Group**, then select the group in the System Tree.

2 Next to **Sorting criteria** click **Edit**. The **Sorting Criteria** page for the selected group appears.

3 Select **Systems that match any of the criteria below**, then the criteria selections appear.

NOTE: Although you can configure multiple sorting criteria for the group, a system only has to match a single criterion to be placed in this group.

4 Configure the criterion. Options include:

- **Tags** — Add specific tags to ensure systems with such tags that come into the parent group are sorted into this group.
- **IP addresses** — Use this text box to define an IP address range or subnet mask as sorting criteria. Any system whose address falls within it is sorted into this group.

5 Repeat as necessary until sorting criteria areconfigured for the group, then click **Save**.

Enabling System Tree sorting on the server

Use this task to enable System Tree sorting on the server. System Tree sorting must be enabled on the server and the desired systems for systems to be sorted.

Task

For option definitions, click **?** on the page displaying the options.

1. Go to **Configuration | Server Settings**, select **System Tree Sorting** in the **Setting Categories** list, then click **Edit**.
2. Select whether to sort systems only on the first agent-server communication or on each agent-server communication.

If you selected to sort only on the first agent-server communication, all enabled systems are sorted on their next agent-server communication and are never sorted again for as long as this option is selected. However, these systems can be sorted again manually by taking the Sort Now action, or by changing this setting to sort on each agent-server communication.

If you selected to sort on each agent-server communication, all enabled systems are sorted at each agent-server communication as long as this option is selected.

Enabling and disabling System Tree Sorting on Systems

Use this task to enable or disable System Tree sorting on systems. The sorting status of a system determines whether it can be sorted into a criteria-based group. Alternatively, you can change the sorting status on systems in any table of systems (such as query results), and also automatically on the results of a scheduled query.

Task

For option definitions, click **?** on the page displaying the options.

1. Go to **Systems | System Tree | Systems**, then select the desired systems.
2. Click **Change Sorting Status**, then select whether to enable or disable System Tree sorting on selected systems.

   NOTE: You may need to click **More Actions** to access the **Change Sorting Status** option. To view the sorting status of systems, add the column to the **Systems** page.

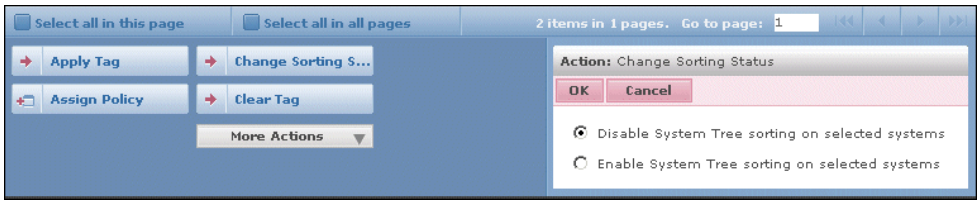

Figure 12: Change Sorting Status options

Depending on the server setting for System Tree sorting, these systems are sorted on the next agent-server communication. Otherwise, they can only be sorted with the Sort Now action.

Sorting systems manually

Use this task to sort selected systems into groups with criteria-based sorting enabled.

Task

For option definitions, click **?** on the page displaying the options.

1 Go to **Systems | System Tree | Systems**, then select the group that contains the desired systems.

2 Select the systems, then click **Sort Now**. You may have to click **More Actions** to access this option. The **Sort Now** dialog box appears.

   NOTE: If you want to preview the results of the sort before sorting, click **Test Sort** instead. (However, if you move systems from within the **Test Sort** page, all selected systems are sorted, even if they have System Tree sorting disabled.)

3 Click **OK** to sort the systems.

Importing Active Directory containers

Use this task to import systems from your network's Active Directory containers directly into your System Tree by mapping Active Directory source containers to the groups of the System Tree. Unlike previous versions, you can now:

- Synchronize the System Tree structure to the Active Directory structure so that when containers are added or removed in Active Directory, the corresponding group in the System Tree is added or removed also.
- Delete systems from the System Tree when they are deleted from Active Directory.
- Prevent duplicate entries of systems in the System Tree when they already exist in other groups.

Before you begin

You must have appropriate permissions to perform this task.

Best practices

Implementation of this feature depends on whether you are creating the System Tree for the first time or if you upgrading from a previous version with an existing System Tree structure with which you are not using Active Directory integration.

If you have been using a previous version of ePolicy Orchestrator and already have a fully-populated System Tree, you can still take advantages of Active Directory integration by mapping your System Tree groups to Active Directory containers. You can use this feature to create mapping points between Active Directory containers and System Tree groups to import any new systems found in Active Directory to the appropriate location of the System Tree.

Task

For option definitions, click **?** on the page displaying the options.

1 Go to **Systems | System Tree | Group**, then select the desired group in the System Tree. This should be the group to which you want to map an Active Directory container.

NOTE: You cannot synchronize the **My Organization** or **Lost&Found** groups of the System Tree.

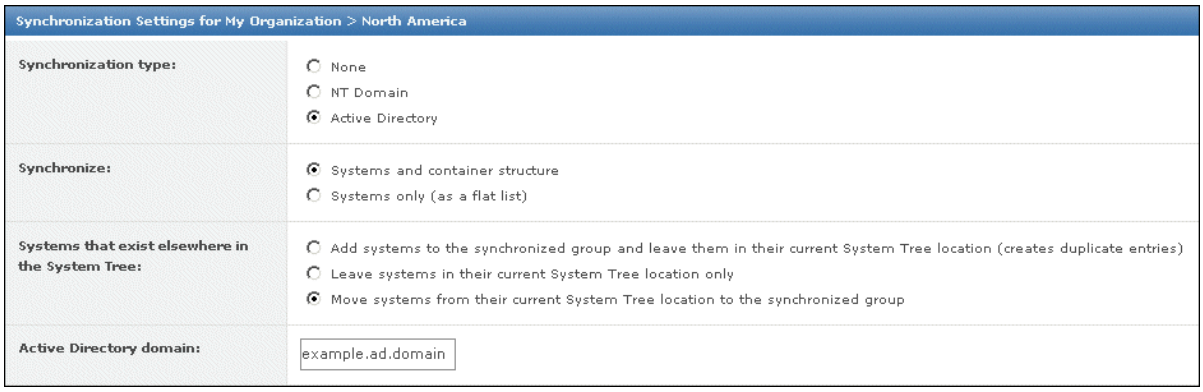
Synchronization Settings for My Organization > North America
Synchronization type:
None
NT Domain
Active Directory
Synchronize:
Systems and container structure
Systems only (as a flat list)
Systems that exist elsewhere in the System Tree:
Add systems to the synchronized group and leave them in their current System Tree location (creates duplicate entries)
Leave systems in their current System Tree location only
Move systems from their current System Tree location to the synchronized group
Active Directory domain:
example.ad.domain

Figure 13: Synchronization Settings page

2 Next to **Synchronization type** click **Edit**. The **Synchronization Settings** page for the selected group appears.

3 Next to **Synchronization type** select **Active Directory**. The Active Directory synchronization options appear.

4 Select the type of Active Directory synchronization you want to occur between this group and the desired Active Directory container (and its subcontainers):

- **Systems and container structure** — Select this option if you want this group to truly reflect the Active Directory structure. When synchronized, the System Tree structure under this group is modified to reflect that of the Active Directory container it's mapped to. When containers are added or removed in Active Directory, they are added or removed in the System Tree. When systems are added, moved, or removed from Active Directory, they are added, moved, or removed from the System Tree.
- **Systems only** — Select this option if you only want the systems from the Active Directory container (and non-excluded subcontainers) to populate this group, and this group only. No subgroups are created like when mirroring Active Directory.

5 Select whether a duplicate entry for the system will be created for a system that already exists in another group of the System Tree.

TIP: McAfee does not recommend selecting this option, especially if you are only using the Active Directory synchronization as a starting point for security management and use other System Tree management functionalities (for example, tag sorting) for further organizational granularity below the mapping point.

6 In **Active Directory domain**, type the fully-qualified domain name of your Active Directory domain.

7 In **Active Directory credentials**, type the Active Directory user credentials that ePolicy Orchestrator uses to retrieve the Active Directory information.

8 Next to **Container**, click **Browse** and select a source container in the **Select Active Directory Container** dialog box, then click **OK**.

9 To exclude specific subcontainers, click **Add** next to **Exclusions** and select a subcontainer to exclude, then click **OK**.

10 Select whether to deploy agents automatically to new systems. If you do, be sure to configure the deployment settings.

TIP: McAfee recommends that you do not deploy the agent during the initial import if the container is large. Deploying the 3.62 MB agent package to many systems at once may cause network traffic issues. Instead, import the container, then deploy the agent to groups of systems at a time, rather than all at once. Consider revisiting this page and selecting this option after the initial agent deployment, so that the agent is installed automatically on new systems added to Active Directory.

11 Select whether to delete systems from the System Tree when they are deleted from the Active Directory domain.

12 To synchronize the group with Active Directory immediately, click **Synchronize Now**. Clicking **Synchronize Now** saves any changes to the synchronization settings before synchronizing the group. If you have an Active Directory synchronization notification rule enabled, an event is generated for each system added or removed (these events appear in the Notfifications Log, and are queryable). If you deployed agents to added systems, the deployment is initiated to each added system. When the synchronization completes,the **Last Synchronization** time is updated, displaying the time and date when the synchronization finished, not when any agent deployments completed.

NOTE: Alternatively, you can schedule an NT Domain/Active Directory Synchronization server task for the first synchronization. This is useful if you are deploying agents to new systems on the first synchronization, when bandwidth is a larger concern.

13 When the synchronization completes, view the results with the System Tree.

Once the systems are imported, distribute agents to them if you did not select to do so automatically. Also, consider setting up a recurring NT Domain/Active Directory Synchronization server task to keep your System Tree up to date with any new systems or organizational changes in your Active Directory containers.

Importing NT domains to an existing group

Use this task to import systems from an NT domain to a group you created manually.

You can populate groups automatically by synchronizing entire NT domains with specified groups. This is an easy way to add all the systems in your network to the System Tree at once as a flat list with no system description.

If the domain is very large, you can create subgroups to assist with policy management or System Tree organization. To do this, first import the domain into a group of your System Tree, then manually create logical subgroups.

TIP: To manage the same policies across several domains, import each of the domains into a subgroup under the same group, on which you can set policies that inherit into each of the subgroups.

When using this method:

- Set up IP address or tag sorting criteria on subgroups to automatically sort the imported systems.
- Schedule a recurring NT Domain/Active Directory Synchronization server task for easy maintenance.

Task

For option definitions, click **?** on the page displaying the options.

1 Go to **Systems | System Tree | Group**, then select or create a group in the System Tree.

2 Next to **Synchronization type**, click **Edit**. The **Synchronization Settings** page for the selected group appears.

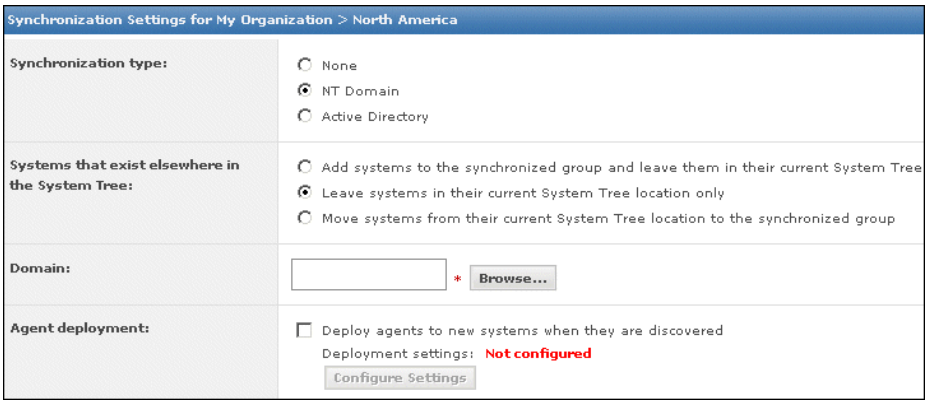
Synchronization Settings for My Organization > North America
Synchronization type:
None
NT Domain
Active Directory
Systems that exist elsewhere in the System Tree:
Add systems to the synchronized group and leave them in their current System Tree
Leave systems in their current System Tree location only
Move systems from their current System Tree location to the synchronized group
Domain:
Browse...
Agent deployment:
Deploy agents to new systems when they are discovered
Deployment settings: Not configured
Configure Settings

Figure 14: Synchronization Settings page

3 Next to **Synchronization type**, select **NT Domain**. The domain synchronization settings appear.

4 Next to **Systems that exist elsewhere in the System Tree**, select what to do with systems that would be added during synchronization already exist in another group of the System Tree.

NOTE: McAfee does not recommend selecting **Add systems to the synchronized group and leave them in their current System Tree location**, especially if you are only using the NT domain synchronization as a starting point for security management and use other System Tree management functionalities (for example, tag sorting) for further organizational granularity below the mapping point.

5 Next to **Domain**, click **Browse** and select the NT domain to map to this group, then click **OK**. Alternatively, you can type the name of the domain directly in the text box.

NOTE: When typing the domain name, do not use the fully-qualified domain name.

6 Select whether to deploy agents automatically to new systems. If you do so, be sure to configure the deployment settings.

TIP: McAfee recommends that you do not deploy the agent during the initial import if the domain is large. Deploying the 3.62 MB agent package to many systems at once may cause network traffic issues. Instead, import the domain, then deploy the agent to smaller groups of systems at a time, rather than all at once. However, once you've finished deploying agents, consider revisiting this page and selecting this option after the initial agent deployment, so that the agent is installed automatically on any new systems that are added to the group (or its subgroups) by domain synchronization.

7 Select whether to delete systems from the System Tree when they are deleted from the NT domain.

8 To synchronize the group with the domain immediately, click **Synchronize Now**, then wait while the systems in the domain are added to the group.

NOTE: Clicking **Synchronize Now** saves changes to the synchronization settings before synchronizing the group. If you have an NT domain synchronization notification rule enabled, an event is generated for each system added or removed. (These events appear in the Notifications Log, and are queryable). If you selected to deploy agents to added systems, the deployment is initiated to each added system. When the synchronization completes, the **Last Synchronization** time is updated. The time and date are when the synchronization finished, not when any agent deployments completed.

9 If you want to synchronize the group with the domain manually, click **Compare and Update**. The **Manually Compare and Update** page appears.

NOTE: Clicking **Compare and Update** saves any changes to the synchronization settings.

a If you are going to remove any systems from the group with this page, select whether to remove their agents when the system is removed.

b Select the systems to add to and remove from the group as necessary, then click **Update Group** to add the selected systems. The **Synchronize Setting** page appears.

10 Click **Save**, then view the results in the System Tree if you clicked **Synchronize Now** or **Update Group**.

Once the systems are added to the System Tree, distribute agents to them if you did not select to deploy agents as part of the synchronization. Also, consider setting up a recurring NT Domain/Active Directory Synchronization server task to keep this group up-to-date with new systems in the NT domain.

Synchronizing the System Tree on a schedule

Use this task to schedule a server task that updates the System Tree with changes in the mapped domain or Active Directory container. Depending on a group's synchronization settings, this task:

- Adds new systems on the network to the specified group.
- Adds new corresponding groups when new Active Directory containers are created.
- Deletes corresponding groups when Active Directory containers are removed.
- Deploys agents to new systems.
- Removes systems that are no longer in the domain or container.
- Applies policies and tasks of the site or group to new systems.
- Prevents or allows duplicate entries of systems that still exist in the System Tree that you've moved to other locations.

NOTE: The agent cannot be deployed to all operating systems in this manner. You might need to distribute the agent manually to some systems.

Task

For option definitions, click **?** on the page displaying the options.

1 Go to **Automation | Server Tasks**, then click **New Task** at the bottom of the page. The **Description** page of the **Server Task Builder** appears.

2 Name the task and choose whether it is enabled once it is created, then click **Next**. The **Actions** page appears.

3 From the drop-down list, select **NT Domain/Active Directory Synchronization**.

4 Select whether to synchronize all groups or selected groups. If you are synchronizing only some synchronized groups, click **Select Synchronized Groups** and select specific ones.

5 Click **Next**. The **Schedule** page appears.

6 Schedule the task, then click **Next**. The **Summary** page appears.

7 Review the task details, then click **Save**.

NOTE: In addition to the task running at the scheduled time, you can run this task immediately by clicking **Run** next to the task on the **Server Tasks** tab.

Updating the synchronized group with an NT domain manually

Use this task to update a synchronized group with its mapped NT domain, including:

- Add systems currently in the domain.
- Remove systems from your System Tree that are no longer in the domain.
- Remove agents from all systems that no longer belong to the specified domain.

Task

For option definitions, click **?** on the page displaying the options.

1 Go to **Systems | System Tree | Group**, then select the group that is mapped to the NT domain.

2 Next to **Synchronization type**, click **Edit**. The **Synchronization Settings** page appears.

3 Near the bottom of the page, click **Compare and Update**. The **Manually Compare and Update** page appears.

4 If you are removing systems from the group, select whether to remove the agents from systems that are removed.

5 Click **Add All** or **Add** to import systems from the network domain to the selected group.

Click **Remove All** or **Remove** to delete systems from the selected group.

6 Click **Update Group** when finished.

Moving systems manually within the System Tree

Use this task to move systems from one group to another in the System Tree. You can move systems from any page that displays a table of systems, including the results of a query.

Even if you have a perfectly organized System Tree that mirrors your network hierarchy, and use automated tasks and tools to regularly synchronize your System Tree, you may need to move systems manually between groups. For example, you may need to periodically move systems from the Lost&Found group.

Task

For option definitions, click **?** on the page displaying the options.

1 Go to **Systems | System Tree | Systems**, then browse to and select the systems.

2 Click **Move Systems**. The **Select New Group** page appears.

NOTE: You may need to click **More Actions** to access this action.

3 Select whether to enable or disable System Tree sorting on the selected systems when they are moved.

4 Select the group in which to place the systems, then click **OK**.

Distributing Agents to Manage Systems

Managing your network systems effectively is dependent on each system running an active, up-to-date agent.

There are several methods to distribute the agent. The ones you use depend on:

- The realities of your environment.
- Whether you are upgrading agents or distributing them for the first time.

Are you distributing agents for the first time?

When deploying agents throughout your environment for the first time:

1. Review the information in this chapter to understand the agent, its policies and tasks, and the methods to distribute it.
2. Configure agent policy settings for the System Tree groups to which you are distributing agents.
3. Distribute agents with the chosen methods to the desired locations.

Contents

- Agents and SuperAgents
- Agent-server communication
- Agent activity logs
- Agent policy settings
- Security Keys
- Methods of agent distribution
- Creating custom agent installation packages
- Distributing agents
- Forcing the agent to call in to the server
- Upgrading existing agents
- Removing the agent
- Maintaining the agent
- Agent command-line options
- Agent installation command-line options

Agents and SuperAgents

The agent is the distributed component of ePolicy Orchestrator that must be installed on each system in your network that you want to manage. A SuperAgent is an agent that is enabled to broadcast wake-up calls by network broadcast segment. SuperAgents can also be used as a repository from which to distribute products and updates.

The agent collects and sends information among the ePO server, update repositories, managed systems, and products. Systems cannot be managed by ePolicy Orchestrator without an installed agent.

Agent installation folder

The location of the agent installation folder differs on managed systems and the server by default.

On the server system, the agent is installed in this location:

<SYSTEM_DRIVE>\PROGRAM FILES\MCAFEE\COMMON FRAMEWORK

On the managed system, if the agent was installed as part of another product installation or pushed from the console to the system, it is installed by default in this location:

<SYSTEM_DRIVE>\PROGRAM FILES\MCAFEE\COMMON FRAMEWORK

On the managed system, if you are upgrading the agent from version 2.5.1, the new agent is also installed after the existing agent is uninstalled, by default in this location:

<SYSTEM_DRIVE>\PROGRAM FILES\NETWORK ASSOCIATES\COMMON FRAMEWORK

CAUTION: Once the agent has been installed, you cannot change its installation directory without first removing it.

Agent language packages

Agent installation packages, both default and custom, install in English. These are in the master repository by default for clean installations.

Each agent language package includes only those files needed to display the user interface in that language. Agent language packages can be replicated to distributed repositories.

After the initial agent-server communication, the agent retrieves the new package that corresponds to the in-use locale and applies it. In this way, the agents retrieve only language packages for the locales being used on each managed system.

NOTE: The interface continues to appear in the current language until the new language package has been applied.

Multiple language packages can be stored on managed systems to allow users to switch languages by changing the locale. If a locale is selected for which a language package is not available locally, the interface appears in English.

Agent language packages are available for these languages:

- Brazilian Portuguese
- Chinese (Simplified)
- Chinese (Traditional)
- English
- Dutch
- French (Standard)
- German (Standard)
- Italian
- Japanese
- Korean
- Polish
- Spanish
- Swedish

The agent installation package

The FRAMEPKG.EXE file is created when you install the server. It is a customized installation package for agents that report to your server. The package contains the server name, its IP address, ASCI port number, and other information that allows the agent to communicate with the server.

By default, the agent installation package is installed in this location:

C:\PROGRAM FILES\MCAFEE\EPO\DB\SOFTWARE\CURRENT\ ePOAGENT3000\INSTALL\0409\FRAMEPKG.EXE

This is the installation package that the server uses to deploy agents.

The default agent installation package contains no embedded user credentials. When executed on the system, the installation uses the account of the currently logged-on user.

Agent-server communication

During agent-server communication, the agent and server exchange information using SPIPE, a proprietary network protocol used by ePolicy Orchestrator for secure network transmissions. At each communication, the agent collects its current system properties, as well as any events, and sends them to the server. The server sends any new or changed policies, tasks, and repository list to the agent. The agent then enforces the new policies locally on the managed system.

Agent-server communication can be initiated in three ways:

- Agent-to-server communication interval (ASCI)
- Agent-initiated communication after agent startup
- Agent wake-up calls
- Communication initiated manually from the managed system

Agent-to-server-communication interval

The agent-to-server-communication interval (ASCI) is set on the **General** tab of the **McAfee Agent** policy pages. This setting determines how often the agent calls into the server for data exchange and updated instructions. By default, the ASCI is set to 60 minutes; the agent checks into the server once every hour.

When deciding whether to modify this policy setting, you must consider your organization's threat response requirements, available bandwidth, and the hardware hosting the server. Be aware that ASCI communication can generate significant network traffic, especially in a large network. In such a case, you probably have agents in remote sites connecting over slower network connections. For these agents, you may want to set a less frequent ASCI. The following table lists general ASCI recommendations for common network connection speeds.

General recommended ASCI settings

Network Size	Recommended ASCI
Gigabit LAN	60 minutes
100mb LAN	60 minutes
WAN	360 minutes
Dial-up or RAS	360 minutes
10mb LAN	180 minutes

Network Size	Recommended ASCI
Wireless LAN	150 minutes

NOTE: For complete information on balancing bandwidth, server hardware, and ASCI determination, see the *ePolicy Orchestrator 4.0.2 Hardware Sizing and Bandwidth Usage Guide*.

Agent-initiated after agent startup

After the installation, and after the agent service is stopped and restarted, the agent calls into the server at a randomized interval within ten minutes. Subsequent communications occur with the ASCI set in the agent policy (60 minutes by default).

You can force the agent to communicate to the server immediately after the installation by running the CMDAGENT.EXE with the /P command-line option.

Wake-up calls

Wake-up calls prompt the agents to call in to the server. Wake-up calls can be sent manually or scheduled as a client task. These are useful when you have made policy changes or checked in updates that you want to apply to the managed systems sooner than the next ASCI.

Wake-up calls can also configured on query results which are scheduled in the Server Task Builder wizard.

SuperAgents and broadcast wake-up calls

If you plan to use agent wake-up calls to initiate agent-server communication, consider converting an agent on each network broadcast segment into a SuperAgent. SuperAgents distribute the bandwidth impact of the agent wake-up call, minimizing network traffic.

Instead of sending agent wake-up calls from the server to every agent, the server sends the SuperAgent wake-up call to SuperAgents in the selected System Tree segment. When SuperAgents receive this wake-up call they send broadcast wake-up calls to all the agents in their network broadcast segments. This reduces network traffic. This is beneficial in large

networks where ePolicy Orchestrator may manage agents in remote sites over lower-speed WAN or VPN connections.

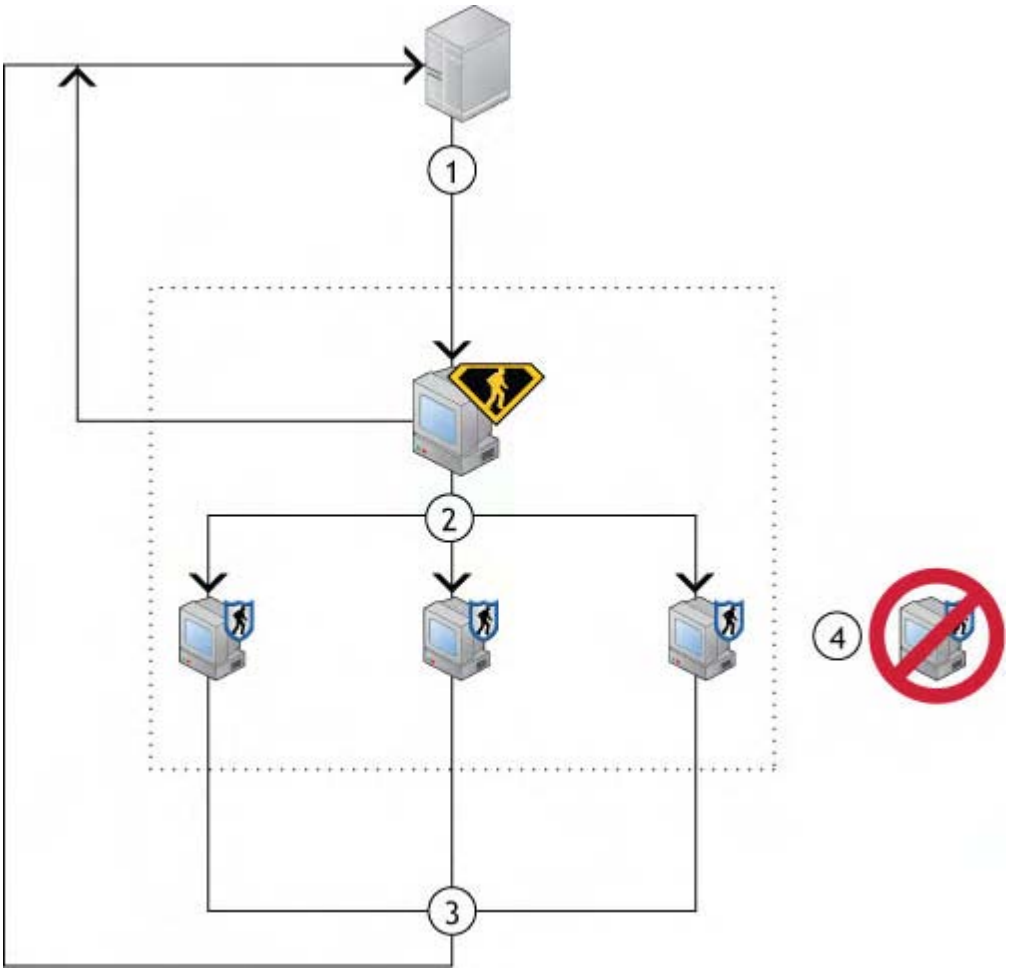

Figure 15: SuperAgent and Broadcast Wake-Up Calls

1 Server sends a wake-up call to all SuperAgents.

2 SuperAgents send a broadcast wake-up call to all agents in the same broadcast segment.

3 All agents (regular agents and SuperAgents) exchange data with the server.

4 Any agents without an operating SuperAgent on its broadcast segment are not prompted to communicate with the server.

Best practices

To deploy sufficient numbers of SuperAgents to the appropriate locations, first determine the broadcast segments in your environment and select a system (preferably a server) in each to host a SuperAgent. Be aware that agents in broadcast segments without SuperAgents do not receive the broadcast wake-up call, and therefore, do not call in to the server.

Similar to the regular agent wake-up call, the SuperAgent wake-up call uses the SPIPE protocol. Ensure the agent wake-up communication port (8081 by default) and the agent broadcast communication port (8082 by default) are not blocked.

Agent activity logs

The agent log files are useful for determining agent status or troubleshooting. Two log files record agent activity, both are located in the agent installation folders on the managed system.

Agent activity log

The agent activity log is an XML file named agent_<system>.xml where <system> is the NetBIOS name of the system on which the agent is installed. This log file records agent activity related to thingssuch as policy enforcement, agent-server communication, and event forwarding. You can define a size limit of this log file.

On the **Logging** tab of the **McAfee Agent** policy pages, you can configure the level of agent activity that is recorded.

Detailed agent activity log

The detailed agent activity log is named agent_<system>.log file where <system> is the NetBIOS name of the system on which the agent is installed. In addition to the information stored in the agent activity log, the detailed activity log contains troubleshooting messages. This file has a 1MB size limit. When this log file reaches 1MB, a backup copy is made (agent_<system>_backup.log).

Agent policy settings

Agent policy settings determine agent performance and behavior in your environment, including:

- How often the agent calls in to the server.
- How often the agent enforces policies on the managed system.
- How often the agent delivers event files to the server.
- Where the agent goes for product and update packages.

Before distributing a large number of agents throughout your network, consider carefully how you want the agent to behave in the segments of your environment. Although you can configure agent policy after agents are distributed, McAfee recommends setting agent policy prior to the distribution to prevent unnecessary resource impact.

For complete descriptions of options on the agent policy pages, click **?** on the page displaying the options. However, some of the most important policy settings are discussed here.

Priority event forwarding

The agent and security software on the managed system generate software events constantly during normal operation. These can range from information events about regular operation, such as when the agent enforces policies locally, to critical events, such as when a virus is detected and not cleaned. These events are sent to the server at each agent-server communication and stored in the database. A typical deployment of ePolicy Orchestrator in a large network can generate thousands of these events an hour. Most likely, you won't want to see each of these.

Typically, you may want to know about higher severity events immediately. You can configure the agent to forward events that are equal to or greater than a specified severity immediately (specific event severities are determined by the product generating the events). If you plan to

use Notifications, enabling immediate uploading of higher severity events is necessary for those features to function as intended.

You can enable immediate uploading of events on the **Events** tab of the **McAfee Agent** policy pages.

Full and minimal properties

The agent sends information from the managed system to the server at each agent-server communication, allowing you to view the properties of individual systems from ePolicy Orchestrator.

The agent sends the complete set of properties during the initial communication. After that, the agent sends only properties that have changed since the last communication.

However, the agent sends the complete set again if:

- Policy is set to send full properties, and enforced on the managed systems.
- Properties versions on the agent and the ePO server differ by more than two.

The properties listed depend on whether you selected to send full or minimal properties on the **General** tab of the **McAfee Agent** policy pages.

Full properties

If you specify to collect the full set of properties, the agent collects:

- System properties:
  - System hardware information.
  - Installed software information.
  - Processor speed.
  - Operating system.
  - Time zone.
  - Most recent date and time that properties were updated.
- Product properties:
  - Installation path.
  - Detection definition (DAT) file version number.
  - Product version number.
  - Specific policy settings configured for each product.

Minimal properties

If you specify to collect only minimal properties, the agent collects only these product properties:

- Installation path.
- Detection definition (DAT) file version number.
- Product version number.
- Specific policy settings configured for each product.

Agent policy and distributed repositories

By default, the agent can update from any repository in its repository list (SITELIST.XML) file. The agent can use a network ICMP ping command or the repository's subnet address to determine the distributed repository with the fastest response time out of the top five repositories in the list. Usually, this is the distributed repository that is closest to the system on the network. For example, a managed system in a remote site far from the ePO server probably selects a local distributed repository. By contrast, an agent in the same LAN as the server probably updates directly from the master repository.

If you require tighter control over which distributed repositories the agents use, you can enable or disable specific distributed repositories on the **Repositories** tab of the McAfee Agent policy pages. Allowing agents to update from any distributed repository ensures they get the update from some location. Using a network ICMP ping, the agent should update from the closest distributed repository from the top five in the repository list.The agent selects a repository each time the agent service (**McAfee Framework Service**) starts or when the repository list changes.

Proxy settings

To access the McAfee update sites, the agent must be able to access the Internet. Use the agent policy settings to configure proxy server settings for the managed systems.The **Proxy** tab of the **McAfee Agent** policy pages includes settings to:

- Use Internet Explorer proxy settings.
- Configure custom proxy settings.
- Disable any proxy use.

The default setting is **Use Internet Explorer Proxy Settings**, allowing an agent to use the current proxy server location and credential information currently configured in the Internet Explorer browser installed on that system.However, you may need to use ePolicy Orchestrator to configure custom proxy server settings for systems in your network. For example, maybe they use a different browser and don't have Internet Explorer installed.

Security Keys

ePolicy Orchestrator and the agents use keys to secure agent-server communication and to sign and validate unsigned packages.

Agents update changes to keys on the next Update client task for the agent.

Agent-server secure communication keys

Agent-server secure communication (ASSC) keys are used by the agents to communicate securely with the server. You can make any ASSC key pair the master, which is the one currently assigned to agents deployed. Exisiting agents using other keys in the list change to the new master after the next update. Be sure to wait until all agents have updated to the new master before deleting older keys.

Agents previous to version 3.6 use a legacy key. If you are upgrading from a previous version of ePolicy Orchestrator, the legacy key may be the master key by default.

Master repository key pair

The master repository private key signs all unsigned content in the master repository. These keys are in anticipation of the McAfee Agent 4.0.

Agents version 4.0 or later use the public key to verify the repository content originating from the master repository on this ePO server. If the content is unsigned, or signed with an unknown repository private key, the downloaded content is considered invalid and deleted.

This key pair is unique to each server installation. However, by exporting and importing keys, you can use the same key pair in a multi-server environment.

These keys are a new feature and only agents 4.0 or later are compliant with the new protocols.

Other repository public keys

These are the public keys that agents use to verify content from other master repositories in your environment or McAfee source sites. Each agent reporting to this server uses the keys in this list to verify content that originates from other ePO servers in your organization, or from McAfee owned sources.

If an agent downloads content that originated from a source for which the agent does not have the appropriate public key, the agent discards the content.

These keys are a new feature and only agents 4.0 or later are able to use the new protocols.

Methods of agent distribution

Due to the variety of scenarios and requirements of different environments, there are several methods you can use to distribute the agent to the systems you want to manage. Before using any of these methods, you should consider each.

The following table details the advantages and disadvantages of the different methods to distribute the agent.

Table 1: Advantages and disadvantages of agent distribution methods

Method	Advantages	Disadvantages
Deploying agents while creating Directory	Automatic; no other steps are required.	If you are creating sites by importing large NT domains or Active Directory containers, too much network traffic may be generated for your resources.
Deploying agents from ePolicy Orchestrator	This is an efficient method for distributing the agent.	You must embed user credentials with administrator rights to the desired systems. Also, you must ensure that systems running Microsoft XP Service Pack 2, have the FRAMEPKG.EXE file added to the firewall exceptions list.
Using login scripts	This is an efficient method for an environment where systems log on to the network frequently. You do the work once, and the agent is deployed automatically.	Systems that don't log on to the network frequently, may not be running the most up-to-date agent.
Installing manually	This is an efficient method if you are not using ePolicy Orchestrator to deploy the agent, or if you have many Windows 95 and Windows 98 systems and do not want to enable file and print sharing on them.	This is not a time-efficient method if you have many systems.

Method	Advantages	Disadvantages
Including the agent on an image	Prevents the bandwidth impact that other forms of distribution can cause. Reduces the overhead by integrating the task into another.	If you do not use images consistently, this method would not be efficient to ensure coverage.
Enabling the agent on unmanaged McAfee products	Saves significant bandwidth and time.	The disabled agent may be out-of-date and require you run the deployment task to upgrade the agent to the current release. You cannot change the agent installation folder without removing and reinstalling the agent. Agents that you enable may be located in a different folder than agents that you deploy in your network by some other method.

Creating custom agent installation packages

Use this task to create a custom agent installation package.

If you use a distribution method other than ePolicy Orchestrator deployment capabilities (such as login scripts or third-party deployment software), you must create a custom agent installation package (FRAMEPKG.EXE) with embedded administrator credentials if users do not have local administrator permissions. The user account credentials you embed are used to install the agent.

NOTE: For Microsoft Windows XP Service Pack 2 and later operating systems do not allow embedded administrator credentials until the package file name has been added to the exception list of the Windows firewall.

Task

For option definitions, click **?** on the page displaying the options.

1. Go to **Systems | System Tree**, then click **New Systems**. The **New Systems** page appears.
2. Next to **How to add systems**, select **Create and download agent installation package**.
3. Type the desired **Credentials for agent installation**, then click **OK**.
4. When prompted, select the location for downloading and saving the installation package.
5. Distribute the custom installation package file as needed.

Distributing agents

Use any of these tasks to distribute agents across your environment. The methods you choose depend on the requirements in your environment.

Tasks

- Deploying the agent with ePolicy Orchestrator
- Installing the agent with login scripts
- Installing the agent manually
- Enabling the agent on unmanaged McAfee products

- Including the agent on an image
- Using other deployment products
- Distributing the agent to WebShield appliances and Novell NetWare servers

Deploying the agent with ePolicy Orchestrator

Use this task to deploy agents to your systems with ePolicy Orchestrator. This method uses Windows NT push technology.

This method is recommended if large segments of your System Tree are already populated. For example, if you created System Tree segments by importing domains or Active Directory containers and you chose not to deploy during the import.

Before you begin

To use this method, several requirements must be met, including:

- Systems must already be added to the System Tree.

  NOTE: If you have not yet created the System Tree, you can deploy the agent installation package to systems at the same time that you are adding groups, and systems to the System Tree. However, McAfee does not recommend this procedure if you are creating your System Tree by importing large NT domains or Active Directory containers. This can generate too much network traffic.

- Specify domain administrator credentials. Domain administrator rights are required on a system to access the default Admin$ shared folder. The ePO server service requires access to this shared folder in order to install agents and other software.
- Verify the ePO server can communicate with the desired systems.

  Before beginning a large agent deployment, use ping commands to verify that the server can communicate with a few systems in each segment of your network.

  If the targeted systems respond to the ping, then ePolicy Orchestrator can reach the segments.

  NOTE: The ability to successfully use ping commands from the ePO server to the managed systems is not required for the agent to communicate with the server after the agent is installed. This is only a useful test for determining if you can deploy agents from the server.

- Verify that the Admin$ share folders on the desired systems are accessible from the server.

  This test also validates your administrator credentials, because you cannot access remote Admin$ shares without administrator rights.

  To access Admin$ shares on desired systems from the ePO server, select **Start | Run**, then type the path to the client Admin$ share by specifying either the system name or IP address.

  If the systems are properly connected over the network, your credentials have sufficient rights, and if the Admin$ shared folder is present, you should see a **Windows Explorer** dialog box.

- Ensure file and print sharing is enabled. This is disabled by default on Windows 95, Windows 98, and Windows ME systems. In addition, if you have systems in your network running these operating systems, make sure they can be managed by ePolicy Orchestrator. By default, these systems do not allow ePO administration. To enable these systems for ePO administration, download VCREDIST.EXE and DCOM 1.3 updates from the Microsoft web site and install them on each client as required.

- Ensure network access is enabled on Windows XP Home systems. Deploy the agent from ePolicy Orchestrator or install a custom agent installation package on systems running Windows XP Home, you must enable network access.

  To enable network access on systems running Windows XP Home, go to **Start | Control Panel | Performance and Maintenance | Administrative Tools | Local Security Policy | Security Settings | Local Policies | Security Options | Network access: Sharing and security model for local accounts**, then select **Classic - local users authenticate as themselves**.

Task

For option definitions, click **?** on the page displaying the options.

1 Go to **Systems | System Tree**, then select the groups or system to which you want to deploy the agent.

2 Click **Deploy Agents**. The **Deploy McAfee Agent** page appears.

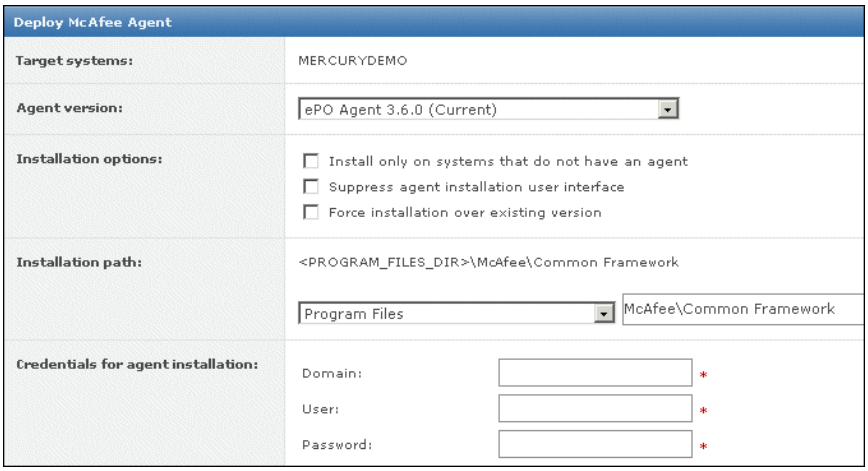

Figure 16: Deploy McAfee Agent page

3 Select the desired **Agent version** from the drop-down list.

4 If you are deploying agents to a group, select whether to include systems from its subgroups.

5 Select whether to:

- **Install only on systems that do not already have an agent managed by this ePO server**
- **Suppress the agent installation user interface**
- **Force installation over existing version**

  This option is not available if **Install only on systems that do not already have an agent managed by this ePO server** is selected.

NOTE: Force installation may be necessary if you experience issues with a new agent and need to re-install the earlier version. This option is recommended for downgrading agents only.

6 Accept the default **Installation path** or select from the drop-down list.

7 Specify **Credentials for agent installation** that have rights to the systems.

8 Click **OK** to send the agent installation package to the selected systems.

Installing the agent with login scripts

Use this task to set up and use network login scripts to install the agent on systems logging on to the network.

Using network login scripts is a reliable method to make sure that every system logging on to your network is running an agent. You can create a login script to call a batch file that checks if the agent is installed on systems attempting to log onto the network. If no agent is present, the batch file can install the agent before allowing the system to log on. Within ten minutes of being installed, the agent calls in to the server for updated policies, and the system is added to the System Tree.

This is a desirable method to use when:

- Sorting filters or NT domain names are assigned to the segments of your System Tree.
- You already have a managed environment and want to ensure that new systems logging on to the network become managed as a result.
- You already have a managed environment and want to ensure systems are running a current version of the agent.

Best practices

McAfee recommends you first create segments of your System Tree that use either network domain names or sorting filters that add the expected systems to the desired groups. If you don't, all systems are added to the **Lost&Found** group and you must move them later manually.

The details of the login script depends on your needs. Consult your operating system documentation for writing login scripts. This task uses a basic example.

Task

For option definitions, click **?** on the page displaying the options.

1. Copy the FRAMEPKG.EXE agent installation package on your server to a shared folder on a network server to which all systems have permissions.

   Systems logging on to the network are directed to this folder to run the agent installation package and install the agent when they log on.

   By default, the agent installation package is in this location:

   C:\PROGRAM FILES\MCAFEE\EPO\DB\SOFTWARE\CURRENT\ ePOAGENT3000\INSTALL\0409\FRAMEPKG.EXE

2. Create a custom agent installation package with embedded administrator user credentials. These credentials are required to install the agent on the system.
3. Create a batch file that contains the lines you want to execute on systems when they log onto the network. The contents of this batch file may differ depending on your needs, but its purpose is to:
   - Check whether the agent has been installed in the expected location.
   - Run FRAMEPKG.EXE if it is not present.

Below is a sample batch file that checks whether the agent is installed and, if it is not, runs the FRAMEPKG.EXE to install the agent.

```
IF EXIST "C:\Windows\System32\ePOAgent\NAIMAS32.EXE"
\\<COMPUTER>\<FOLDER>\UPDATE$\FRAMEPKG.EXE /FORCEINSTALL /INSTALL=AGENT
IF EXIST "C:\ePOAgent\FRAMEWORKSERVICE.EXE" GOTO END_BATCH
\\MyServer\Agent\UPDATE$\FRAMEPKG.EXE /FORCEINSTALL /INSTALL=AGENT
:END_BATCH
```

NOTE: The installation folders for your distribution may be different than in this example, depending on where you have specified to install the agent.

This example checks:

- The default installation location of the older agent version 2.5.1 and, if present, upgrades it to the agent version 3.5.
- The default installation folder for the agent version 3.5 and, if not present, installs the new agent.

4 Save the EPO.BAT batch file to the NETLOGON$ folder of your primary domain controller (PDC) server. The batch file runs from the PDC every time a system logs on to the network.

5 Add a line to your login script that calls the batch file on your PDC server. This line would look similar to this example:

```
CALL \\PDC\NETLOGON$\EPO.BAT
```

Each system runs the script and installs the agent when it logs on to the network.

Installing the agent manually

Use this task to run the installer locally on a system.

This is a desirable method to install agents for the following circumstances:

- Your organization requires that software is installed on systems manually.
- You intend to use ePolicy Orchestrator for policy management only.
- You have systems running Windows 95, Windows 98, or Windows ME and do not want to enable file and print sharing on them.
- You assigned sorting filters or NT domain names when creating the segments of your System Tree.

You can install the agent on the system, or distribute the FRAMEPKG.EXE installer for users to run the installation program themselves.

After the agent is installed, it calls into the server and adds the new system to the System Tree.

Task

For option definitions, click **?** on the page displaying the options.

1 Distribute the agent installation package to the desired system.

If you want end-users (who have local administrator rights) to install the agent on their own systems, distribute the agent installation package file to them. You can attach it to an email message, copy it to media, or save it to a shared network folder.

2 Double-click FRAMEPKG.EXE and wait a few moments while the agent is installed. Within ten minutes, the agent calls in to the ePO server for the first time.

3 As needed, bypass the ten-minute interval by forcing the agent to call in with the CMDAGENT/p command line.

Enabling the agent on unmanaged McAfee products

Use this task to enable agents on existing McAfee products in your environment.

Before purchasing ePolicy Orchestrator, you may have already been using McAfee Enterprise products in your network. Some of the more recent McAfee products that use the AutoUpdate updater, such as VirusScan Enterprise, install with the agent in a disabled state. To start managing these products with ePolicy Orchestrator, you can enable the agent that is already on the system.

Enabling the agent on each system instead of deploying the 3.63MB agent installation package saves significant network bandwidth.

NOTE: You cannot change the agent installation folder without removing and reinstalling the agent. Agents that you enable may be in a different folder than agents that you deploy in your network by another method.

Assigning sorting filters or NT domain names to the desired System Tree segments saves valuable time.

You must copy the SITELIST.XML repository list file from the ePO server to the desired systems. The repository list contains network address information the agent requires to call in to the server after being installed.

Task

For option definitions, click **?** on the page displaying the options.

1. Export the repository list (SITELIST.XML) from the **Master Repository** page to a temporary folder on the system, such as C:\TEMP.
2. Run this command on the desired system:
   FRMINST.EXE /INSTALL=AGENT /SITEINFO=C:\TEMP\SITELIST.XML

   /SITEINFO is the location of the SITELIST.XML file that you exported.

   Reference the SITELIST.XML file in the temporary folder. By default, the FRMINST.EXE file is installed in this location:

   C:\PROGRAM FILES\MCAFEE\COMMON FRAMEWORK

   NOTE: Existing McAfee products were most likely installed with an older version of the agent. These agents are *not* automatically upgraded to the latest version that is on the ePO server. Enable and run a deployment task configured to upgrade the enabled agent on the managed system.

Including the agent on an image

Use this information to install the agent using an image. The first time the user logs on to a system built using a common image that includes the agent, the system is assigned a unique ID called a *global unique identifier* (GUID).

CAUTION: Before creating an image for this purpose, remove the agent GUID registry value from the agent registry key. A GUID is regenerated on the first ASCI with the ePO server.

This is a desirable method to use when:

- Your organization uses standard installation images for new systems.
- You have access to some systems in your environment only when they are brought in for repair.

For instructions, see the documentation for your preferred image-creation product.

Using other deployment products

You may already use other network deployment products to deploy software. You can use many of these tools, such as Microsoft Systems Management Server (SMS), IBM Tivoli, or Novell ZENworks, to deploy agents. Configure your deployment tool of choice to distribute the FRAMEPKG.EXE agent installation package located on your ePO server.

For instructions, see the documentation of the desired deployment tool.

Distributing the agent to WebShield appliances and Novell NetWare servers

You cannot use ePolicy Orchestrator to deploy agents to WebShield® appliances or Novell NetWare servers. Instead, use a login script or manual installation.

These systems require different agents, which can be downloaded from the McAfee web site. These agent installation packages are not installed on the ePO server by default.

See your product documentation for details.

Forcing the agent to call in to the server

Use this task to force the new agent to call into the ePO server immediately. You can do this from any system on which an agent has just been installed. This is useful after installing the agent manually.

Task

For option definitions, click **?** on the page displaying the options.

1. From the system where you just installed the agent, open a DOS command window by selecting **Start** | **Run**, type command, and press **Enter**.
2. In the command window, navigate to the agent installation folder containing the CMDAGENT.EXE file.
3. Type this command.
   CMDAGENT /p
4. Press **Enter**. The agent calls into the server immediately.

When the agent calls in to the server for the first time, the system is added to the System Tree as a managed system. If you configured criteria-based sorting for the System Tree, the system is added to the location appropriate for its IP address or tags. Otherwise, the system is added to the **Lost&Found** group. Once the system is added to the System Tree, you can manage its policies through ePollicy Orchestrator.

Upgrading existing agents

Use these tasks to upgrade existing agents in your environment.

If you have been using an older version of ePolicy Orchestrator and have previous agent versions in your environment, you can upgrade those agents once you've installed your ePO server. The procedure for upgrading the agent depends on which previous agent version is running on your managed systems.

NOTE: Some previous agent versions are not fully functional in ePolicy Orchestrator 4.0.2. For full agent functionality, upgrade to agent version 3.6 Patch 1 or later.

Tasks

- Upgrading agents using login scripts or manual installation
- Upgrading agents with ePolicy Orchestrator

Upgrading agents using login scripts or manual installation

If you don't use ePolicy Orchestrator to deploy agents or products to managed systems, you can use your preferred agent distribution method to upgrade existing agents. Upgrading agents without using ePolicy Orchestrator, such as upgrading manually or using network login scripts, is the same as installing agents for the first time. You must distribute the FRAMEPKG.EXE installation file and launch it on the system using your preferred method.

Upgrading agents with ePolicy Orchestrator

Use this task to upgrade existing agents with the Product Deployment client task. This method provides more control over where and when the upgrade occurs. This is the same deployment task that can be used to deploy products such as VirusScan Enterprise to systems that are already running agents.

Best practices information

You can use the deployment task to upgrade agents. McAfee releases newer versions of the agent periodically. You can deploy and manage these newer versions of the agent with ePolicy Orchestrator. When available, you can download the agent installation package from the McAfee update site and check it into the master repository. Then use the deployment task to upgrade the agents.

CAUTION: Upgrading the agent using the deployment task is not the same as updating an existing agent using the Update client task. Upgrading the agent is for installing a new version of the agent over an older one, such as installing the agent version 3.6 over the version 3.0. The update task is used to update an existing version of the agent with additional updates, such as DAT files and patches, or updating the agent version 3.0.1 to version 3.0.2.

Task

For option definitions, click **?** on the page containing the options.

1. Ensure that the desired agent installation package is checked into the master software repository.
2. Go to **Systems | System Tree | Client Tasks**, then select a portion of the System Tree for which you want to upgrade the agent.
3. Click **New Task**. The **Description** page of the **Client Task Builder** wizard appears.
4. Name the task, select **Product Deployment (McAfee Agent)** from the drop-down lists, then click **Next**. The **Configuration** page appears.

5 Select the agent version from the drop-down list.
6 Select **Install** from the **Action** drop-down list.
7 Add any command-line options.
8 Select whether to run the task at each policy enforcement interval.
9 Select whether to run an update task after successful deployments, then click **Next**.
10 Schedule the task as needed, then click **Next**. The **Summary** page appears.
11 Verify the task's details, then click **Save**.

The task is added to the list of client tasks everywhere it's assigned in the System Tree.

Removing the agent

Use these tasks to remove agents from systems.

NOTE: You cannot remove the agent using the Product Deployment task, which is used to remove products such as VirusScan Enterprise.

Tasks

- Running FRMINST.EXE from a command line
- Removing agents when deleting systems from the System Tree
- Removing agents when deleting groups from the System Tree
- Removing agents from systems in query results

Running FRMINST.EXE from a command line

Use this task to remove the agent from a command line.

Task

- Run the agent installation (FRMINST.EXE) program with the /REMOVE=AGENT command-line option. By default this file is located at:

  C:\PROGRAM FILES\MCAFEE\COMMON FRAMEWORK

Removing agents when deleting systems from the System Tree

Use this task to remove agents from systems that you are deleting from the System Tree.

Task

For option definitions, click **?** on the page displaying the options.

1 Go to **Systems | System Tree | Systems**, then select the group under **System Tree** that contains the systems you want to delete.
2 Select the systems from the list, then click **Delete** at the bottom of the page (you may need to first click **More Actions**).
3 In the **Action** panel, select **Remove agent**, then click **OK**.

The selected systems are deleted from the System Tree and their agents are removed at their next agent-server communication.

Removing agents when deleting groups from the System Tree

Use this task to remove agents from all systems in a group, which you are deleting from the System Tree.

CAUTION: When you delete a group, all child groups and systems are also deleted. If you select the **Remove agents from all systems** checkbox when deleting systems, ePolicy Orchestrator removes the agents from all child systems.

Task

For option definitions, click **?** on the page displaying the options.

1 Go to **Systems | System Tree | Groups**, then select the desired group under **System Tree**.

2 Click **Delete Group** at the bottom of the page (you may need to first click **More Actions**). The **Delete Group** dialog box appears.

3 Select **Remove agent from all systems**, then click **OK**.

The selected systems are deleted from the System Tree and their agents are removed at their next agent-server communication.

Removing agents from systems in query results

Use this task to remove agents from systems listed in the results of queries (for example, the Agent Versions Summary query).

Task

For option definitions, click **?** on the page displaying the options.

1 Run the desired query.

2 Select systems from the query results, then click **Delete** at the bottom of the page.

3 In the **Action** panel, click **Yes** when prompted whether to remove the agent.

The agent is uninstalled after the next agent-server communication.

Maintaining the agent

Use these tasks to ensure agents in your environment are up-to-date and functioning as expected. You may need to perform these tasks on a regular basis.

Tasks

- Sending manual wake-up calls to systems
- Sending manual wake-up calls to a group
- Sending wake-up calls on a schedule
- Viewing the agent activity log
- Viewing of the agent and product properties
- Running agent tasks from the managed system
- Working with security keys

Sending manual wake-up calls to systems

Use this task to manually send an agent or SuperAgent wake-up call to systems in the System Tree. This is useful when you make policy changes and you want agents to call in for an update.

Before you begin

Before sending the agent wake-up call to systems, make sure that wake-up support for the systems' groups is enabled and applied on the **General** tab of the **McAfee Agent** policy pages (enabled by default).

Task

For option definitions, click **?** on the page displaying the options.

1 Go to **Systems | System Tree | Systems**, then select the group that contains the systems.

2 Select the systems from the list, then click **Wake Up Agents**. The **Wake Up McAfee Agent** page appears.

NOTE: You may need to click **More Actions** to expose this action.

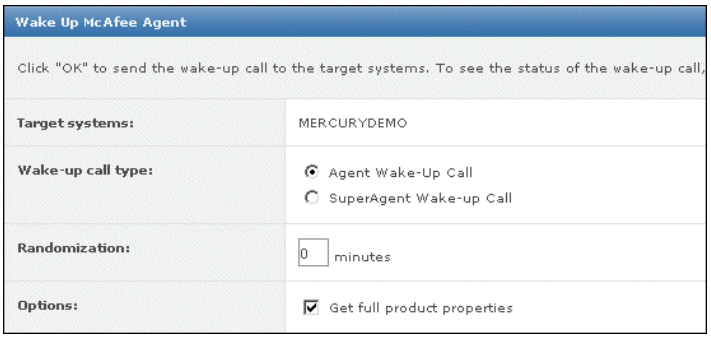

Figure 17: Wake Up McAfee Agent page

3 Verify the systems appear next to **Target systems**.

4 Select whether to send an **Agent Wake-Up Call** or **SuperAgent Wake-Up call** next to **Wake-up call type**.

5 Accept the default or type a different **Randomization** (0 - 60 minutes). Consider carefully the number of systems that are receiving the wake-up call with how much bandwidth is available. If you type 0, agents respond immediately.

6 During regular communication, the agent sends only properties that have changed since the last agent-server communication. This task is set by default to **Get full product properties**. To send the complete properties as a result of this wake-up call, ensure this is option selected.

7 Click **OK** to send the agent or SuperAgent wake-up call.

Sending manual wake-up calls to a group

Use this task to manually send an agent or SuperAgent wake-up call to a System Tree group. This is useful when you have made policy changes and you want agents to call in for an update.

Before you begin

Before sending the agent wake-up call to such a group, make sure that wake-up support for the group is enabled and applied on the **General** tab of the **McAfee Agent** policy pages (enabled by default).

Task

For option definitions, click **?** on the page displaying the options.

1. Go to **Systems | System Tree | Groups**, then select the group under **System Tree**.
2. Click **Wake Up Agents**. The **Wake Up McAfeeAgent** page appears.

   NOTE: You may need to click **More Actions** to expose this action.

3. Verify the group appears next to **Target group**.
4. Select whether to send the agent wake-up call to **All systems in this group** or to **All systems in this group and subgroups**.
5. Select whether to send an **Agent wake-up call** or **SuperAgent wake-up call** next to **Type**.
6. Accept the default or type a different **Randomization** (0 - 60 minutes). If you type 0, agents respond immediately.
7. During regular communication, the agent sends only properties that have changed since the last agent-server communication. This task is set by default to **Get full product properties**. To send the complete properties as a result of this wake-up call, ensure this is option selected.
8. Click **OK** to send the agent or SuperAgent wake-up call.

Sending wake-up calls on a schedule

Use this task to create a scheduled agent wake-up call.

NOTE: SuperAgent wake-up calls cannot be scheduled.

Task

For option definitions, click **?** on the page displaying the options.

1. Go to **Systems | System Tree | Client Tasks**, then select the group or systems to send the wake-up call.
2. Click **New Task**. The **Description** page of the **Client Task Builder** wizard appears.
3. Name the task, select and **Agent Wake-up Call (McAfee Agent)** from the drop-down list, then click **Next**. The **Configuration** page appears.
4. Select whether the agents that receive the wake-up call send full or minimal properties, then click **Next**.
5. Schedule the task as needed, then click **Next**. The **Summary** page appears.
6. Verify the task's details, then click **Save**.

When complete, the scheduled task appears in the list of available tasks on the **Client Tasks** tab of the selected System Tree group. If the task is enabled, it runs at the next scheduled time on systems that have received the task. To ensure all desired systems have the task information, send a manual wake-up call to them.

Viewing the agent activity log

Use these tasks to view the agent activity log. The agent activity log records an agent's activity. The amount of detail depends on the policy settings you selected on the **Logging** tab of the **McAfee Agent** policy pages.

These log files can be viewed from the managed system or from the console.

Tasks

- Viewing the agent activity log from the managed system
- Viewing the agent activity log from the ePO server

Viewing the agent activity log from the managed system

Use this task to view the agent activity log from the system on which the agent is installed.

Task

For option definitions, click **?** on the page that displays the options.

1. Right-click the agent icon in the system tray.

   NOTE: The agent icon is available in the system tray only if the **Show McAfee system tray icon (Windows only)** option is selected on the **General** tab of the **McAfee Agent** policy pages. If it is not visible, select this option and apply it. When you finish viewing the log file content, you can hide the icon again by deselecting the option and applying the change.

2. Select **Status Monitor** from the menu. The status monitor appears, the agent activity log is displayed.
3. Close the status monitor when finished.

Viewing the agent activity log from the ePO server

Use this task to view agent activity log of a system from the server.

Task

For option definitions, click **?** on the page displaying the options.

1. Go to **Systems | System Tree | Systems**, then select the system.
2. Click **View Agent Log**.
3. To view the backup copy of the FrameSvc.exe or NaPrdMgr.exe detailed log, click **previous**.

   NOTE: Although remote viewing of log files is enabled by default, you can disable remote viewing of the log files. If you can't view the log remotely, verify that the **Enable remote access to log** option is selected on the **Logging** tab of the **McAfee Agent** policy pages.

Viewing of the agent and product properties

Use this task to verify that the properties match the policy changes you have made. This is useful for troubleshooting. The properties available depend on whether you configured the agent to send full or minimal properties on the **McAfee Agent** policy pages.

Task

For option definitions, click **?** on the page displaying the options.

1 Go to **Systems | System Tree | Systems**, then select the system.

2 Click the system in the list. Properties for the system, installed products, and the agent appear.

Running agent tasks from the managed system

Use these tasks to perform selected tasks from the system where the agent is installed.

If you can access the managed system where the agent is installed, you can view and manage some features of the agent.

NOTE: The agent interface is available on the managed system only if you selected **Show McAfee system tray icon** on the **General** tab of the **McAfee Agent** policy pages.

Tasks

- Running an update manually
- Sending full properties to the ePO server
- Sending events to the ePO server immediately
- Updating policies
- Enforcing policies
- Viewing agent settings
- Viewing agent and product version numbers

Running an update manually

Use this task to run an update from the managed system.

Task

1 Right-click the McAfee tray icon.

2 Select **McAfee Agent | Update Now.** The agent performs an update from repository determined in the agent policy.

Product updates include:

- Patch releases.
- Legacy product plug-in (.DLL) files.
- Service pack releases.
- SuperDAT (SDAT*.EXE) packages.
- Supplemental detection definition (EXTRA.DAT) files.
- Detection definition (DAT) files.

Sending full properties to the ePO server

Use this task to send full properties to the server from the managed system.

Task

1 Right-click the McAfee tray icon at the managed system, then select **McAfee Agent | Status Monitor**. The **Agent Status Monitor** appears.

2 Click **Collect and Send Props**.

Sending events to the ePO server immediately

Use this task to send events to the server immediately from the managed system.

Task

1 Right-click the McAfee tray icon at the managed system, then select **McAfee Agent | Status Monitor**. The **Agent Status Monitor** appears.

2 Click **Send Events**.

Updating policies

Use this task to prompt the agent from the managed system to call in to the server to update policy settings.

Task

1 Right-click the McAfee tray icon on the desired system, then select **McAfee Agent | Status Monitor**. The **Agent Status Monitor** appears.

2 Click **Check New Policies**.

Enforcing policies

Use this task to prompt an agent to enforce all configured policies on the managed system.

Task

1 Right-click the McAfee tray icon on the desired system, and select **McAfee Agent | Status Monitor**. The **Agent Status Monitor** appears.

2 Click **Enforce Policies**.

Viewing agent settings

Use this task to view the agent settings from the managed system.

Task

1 Right-click the McAfee tray icon at the managed system.

2 Select **McAfee Agent | Settings**.
Agent settings include:

- Agent ID (GUID).
- System name.
- User name of the logged-on user.
- Policy enforcement interval.
- ASCI.

Viewing agent and product version numbers

Use this procedure to look up the agent and product version numbers from the managed system. This is useful for troubleshooting when installing new agent versions or confirming that the installed agent is the same version as the one displayed in the agent properties on the server.

Task

1 Right-click the McAfee tray icon.

2 Select **McAfee Agent | About**.

Working with security keys

Use these tasks to work with and manage security keys.

Tasks

- Using ASSC keys in multi-server environments
- Generating and using new ASSC keys
- Exporting ASSC keys to allow agents to access multiple ePO servers
- Viewing systems that use an ASSC key pair
- Making an ASSC key pair the master
- Deleting ASSC keys
- Using master repository keys in multi-server environments
- Backing up and restoring security keys

Using ASSC keys in multi-server environments

Use either of these tasks to ensure that all agents can communicate with any required server in the environment.

Previous versions of ePolicy Orchestrator allowed agents to easily roam among multiple ePO servers within an organization. Importing ASSC keys into other ePO servers allows agents version 3.6 or later that are managed by source ePO server to successfully communicate with these other ePO servers.

Two strategies ensure agents can communicate with multiple servers. Use a common master ASSC key pair for all ePO servers, or use a different master ASSC key pair for each ePO server and make each server aware of the other servers' keys.

Tasks

- Using the same ASSC key pair for all servers and agents
- Using a different ASSC key pair per ePO server

Using the same ASSC key pair for all servers and agents

Use this task to ensure that all ePO servers and agents use the same ASSC key pair.

Task

For option definitions, click **?** on the page displaying the options.

1 Export the desired ASSC keys from the desired ePO server.
2 Import the ASSC keys to all other servers.
3 Make the imported key the master on all servers.
4 Run an agent update task so that all agents begin using the keys immediately.
5 When all agents are using the new keys, delete any unused keys.
6 Back up all keys.

Using a different ASSC key pair per ePO server

Use this task to ensure all agents can communicate with any required server in an environment where each ePO server is required to have a unique ASSC key pair.

You can ensure that agents can communicate with multiple servers by importing the necessary key pairs into all servers with which the agents may communicate.

Task

For option definitions, click **?** on the page displaying the options.

1 Export the master ASSC key pair from each ePO server in your environment.
2 Import each of these key pairs into every server.

Generating and using new ASSC keys

Use this task to generate new agent-server secure communication (ASSC) keys. Do this if you discover a key has been compromised. McAfee recommends creating and using new ASSC keys routinely, for example every three months.

Task

For option definitions, click **?** on the page displaying them.

1 Go to **Configuration | Server Settings**, then select **Security Keys** in the **Setting Categories** list.
2 Click **Edit** in the details pane. The **Edit Security Keys** page appears.
3 Click **New Key** next to the **Agent-server secure communication keys** list
4 When you want agents to use the new key, select the key in the list, then click **Make Master**.

   Agents version 3.6 or later begin using the new key at the first agent-server communication after their next update task completes.

5 Delete the old key only after all agents have stopped using it.

   To the right of every key in the list is the number of agents currently using it.

6 Back up all keys.

Exporting ASSC keys to allow agents to access multiple ePO servers

Use this task to export ASSC keys for use by other ePO servers in your environment.

Task

For option definitions, click **?** on the page displaying the options.

1 Go to **Configuration | Server Settings**, then select **Security Keys** in the **Setting Categories** list.
2 In the details pane, click **Edit**.
3 In the **Agent-server secure communication keys** list, select the desired key, then click **Export**. The **Export Agent-Server Communication Keys** dialog box appears.
4 Click **OK**. The **File Download** dialog box appears.
5 Click **Save**, then browse to a location to save the ZIP file.
6 Change the name of the file as needed, then click **Save**.

Viewing systems that use an ASSC key pair

Use this task to view the systems whose agents use a specific ASSC key pair in the **Agent-server secure communication keys** list. You may want to view the systems still using the previous key pair after making a different key pair the master. Do not delete a key pair until you know that no agents are still using it.

Task

For option definitions, click ? on the page displaying the options.

1 Go to **Configuration | Server Settings**, select **Security Keys** from the **Setting Categories** list, then click **Edit**.
2 In the **Agent-server secure communication keys** list, select the desired key, then click **View Agents**.

The **Systems Using ASSC Key Pair** page appears. This page displays a standard table listing all of the systems whose agents are using the selected keys. Click any system in the list to view its details, or select the checkboxes next to desired systems and take any of the actions available below the table.

Making an ASSC key pair the master

Use this task to make another key pair listed in the **Agent-server secure communication keys** list the master. Do this after importing or generating a new key pair.

Make the Legacy key pair the master only if you don't have any agents 3.6 or later in your environment. Later versions cannot use the legacy key pair.

Task

For option definitions, click **?** on the page displaying the options.

1 Go to **Configuration | Server Settings**, select **Security Keys** from the **Setting Categories** list, then click **Edit**.
2 Select the desired key from the **Agent-server secure communication keys** list, then click **Make Master**.
3 As needed, create an update task for the agents to run immediately, so that agents update after the next agent-server communication.

   NOTE: Before deleting the previous master key pair from the list, wait until all agents begin using the new master key pair. Agents begin using the new key pair after the next update task for the agent completes. At any time, you can see which agents are using any of the ASSC key pairs in the list.

4 Back up all keys.

Deleting ASSC keys

Use this task to delete unused ASSC keys in the **Agent-server secure communication keys** list.

CAUTION: Do not delete any keys that are currently in use by any agents, or those agents are not able to communicate with the server.

Task

For option definitions, click **?** on the page displaying the options.

1 Go to **Configuration | Server Settings**, select **Security Keys** from the **Setting Categories** list, then click **Edit**.

2 Select the desired key in the **Agent-server secure communication keys** list, then click **Delete**. The **Delete Key** dialog box appears.

3 Click **OK** to delete the key pair from this server.

Using master repository keys in multi-server environments

Use these tasks to ensure agents version 3.6 or later can use content originating from any ePO server in your environment.

The server signs all unsigned content that is checked in to the repository with the master repository private key. Agents use the master repository public key to validate content retrieved from repositories in your organization or McAfee source sites.

The master repository key pair is unique for each installation. If you use multiple servers, each uses a different key. If your agents may download content that originates from different master repositories, you must ensure that agents (version 4.0 or later) recognize the content as valid.

You can ensure this in two ways:

- Use the same master repository key pair for all servers and agents.
- Ensure agents are configured to recognize any repository public key used in your environment.

Tasks

- Using one master repository key pair for all servers
- Ensuring agents can use content from other ePO servers

Using one master repository key pair for all servers

Use this task to ensure all ePO servers and agents use the same master repository key pair in a multi-server environment.

Task

For option definitions, click **?** on the page displaying the options.

1 Go to **Configuration | Server Settings** on the server whose SC key pair you want to use for all servers in your environment, select **Security Keys** in the **Setting Categories** list, then click **Edit**.

2 Next to **Local master repository key pair**, click **Export Key Pair**. The **Export Master Repository Key Pa**ir dialog box appears.

3 Click **OK**. The **File Download** dialog box appears.

4 Click **Save**. The **Save As** dialog box appears.

5 Browse to the location to which to save the ZIP file containing the SC key files. This should be a location accessible by the other servers, then click **Save**.

6 Go to **Configuration | Server Settings** on other servers in your environment, select **Security Keys** in the **Setting Categories** list, then click **Edit**.

7 Click **Import** next to **Import and back up keys**. The **Import Keys** wizard appears.

8 Browse to the ZIP file containing the exported master repository key files, then click **Next**.

9 Verify these are the keys you want to import, then click **Save**.

The imported master repository key pair replaces the existing master repository key pair. Agents begin using the master repository key pair at the next agent update task.

Ensuring agents can use content from other ePO servers

Use this task to ensure agents can use content originating from other ePO servers in a multi-server environment when each server uses a different master repository key.

Task

For option definitions, click **?** on the page displaying the options.

1 Go to **Configuration | Server Settings** on each server in your environment, select **Security Keys** in the **Setting Categories** list, then click **Edit**.

2 Next to **Local master repository key pair**, click **Export Public Key**. The **Export Master Repository Public Key** dialog box appears.

3 Click **OK**. The **File Download** dialog box appears.

4 Click **Save**. The **Save As** dialog box appears.

5 Browse to a location to which to save the ZIP file containing the key files. This should be a location that is accessible to the other servers, then click **Save**.

6 After exporting the public key from each server, go to **Configuration | Server Settings** on each server, select **Security Keys** in the **Setting Categories** list, then click **Edit**.

7 Click **Import**, next to **Import and back up keys**. The **Import Keys** dialog box appears.

8 Browse to the location containing the exported ZIP files, select one, then click **Next**.

9 Verify this is the desired master repository public key, then click **Save**.

10 Repeat until all master repository public keys used in your environment have been imported into each server.

After the next agent update task completes, agents recognize content signed by master repository private keys across your environment.

Backing up and restoring security keys

Use these tasks to back up and restore the security keys. McAfee recommends periodically backing up all of the security keys and storing them in a secure network location so that they can be restored easily in the unexpected event any are lost from the ePO server.

NOTE: McAfee recommends backing up all keys before making any changes to the key management settings.

Tasks

- Backing up all security keys
- Restoring security keys from a backup file

Backing up all security keys

Use this task to back up all security keys currently managed on this ePO server.

Task

For option definitions, click **?** on the page displaying the options.

1. Go to **Configuration | Server Settings**, select **Security Keys** from the **Setting Categories** list, then click **Edit**. The **Edit Security Keys** page appears.
2. Click **Back Up All** near the bottom of the page. The **File Download** dialog box appears.
3. Click **Save**. The **Save As** dialog box appears.
4. Browse to a secure network location to store the ZIP file, then click **Save**.

Restoring security keys from a backup file

Use this task to restore all security keys from a backup file.

Before you begin

You must have already created a backup ZIP file of all of your keys.

CAUTION: When you restore security keys, all existing keys are removed and replaced by the keys in the backup ZIP file. Ensure the needed keys are in the backup file.

Task

For option definitions, click **?** on the page displaying the options.

1. Go to **Configuration | Server Settings**, select **Security Keys** from the **Setting Categories** list, then click **Edit**. The **Edit Security Keys** page appears.
2. Click **Restore All** at the bottom of the page. The **Restore Security Keys** wizard appears.
3. Browse to and select the backup ZIP file, then click **Next**.
4. Verify the keys in this file are the ones you want to overwrite your existing keys, then click **Restore**.

Agent command-line options

Use the Command Agent (CMDAGENT.EXE) tool to perform selected agent tasks from the managed system. CMDAGENT.EXE is installed on the managed system at the time of agent installation. Perform this task locally on managed systems using this program or the McAfee tray icon.

The CMDAGENT.EXE file is located in the agent installation folder. By default, this location is:

C:\PROGRAM FILES\MCAFEE\COMMON FRAMEWORK

Option definitions

Option	Description
/C	Checks for new policies. The agent contacts the ePO server for new or updated policies, then enforces them immediately upon receipt.
/E	Prompt the agent to enforce policies locally.
/P	Send properties and events to the ePO server.
/S	Displays the agent monitor.

Agent installation command-line options

Depending on whether the agent is already installed, use command-line options when you run the agent installation package (FRAMEPKG.EXE) or the agent framework installation (FRMINST.EXE) program.

You can employ these command-line options when using the deployment task to upgrade to a new version of the agent.

This table describes all of the agent installation command-line options. These options are *not* case-sensitive, but their values are.

FRAMEPKG.EXE and FRMINST.EXE command-line options

Command	Description
/DATADIR	Specifies the folder on the system to store agent data files. The default location is: <Documents and Settings>\All Users\Application Data\McAfee\Common Framework.If the operating system not have a Documents and Settings folder, the default location is the Data folder within the agent installation folder. Sample: FRAMEPKG /INSTALL=AGENT /DATADIR=<AGENT DATA PATH>
/DOMAIN/USERNAME/PASSWORD	Specifies an NT domain, and account credentials used to install the agent. The account must have rights to create and start services on the desired system. If left unspecified, the credentials of the currently logged-on account are used. If you want to use an account that is local to the desired system, use the system's name as the domain. Sample: FRAMEPKG /INSTALL=AGENT /DOMAIN=Domain1 /USERNAME=jdoe /PASSWORD=password
/FORCEINSTALL	Specifies that the existing agent is uninstalled, then the new agent is installed. Use this option only to change the installation directory or to downgrade the agent. When using this option, McAfee recommends specifying a different directory for the new installation (/INSTDIR).

Command	Description
	Sample: FRAMEPKG /INSTALL=AGENT /FORCEINSTALL /INSTDIR=c:newagentdirectory
/INSTALL=AGENT	Installs and enables the agent. Sample: FRAMEPKG /INSTALL=AGENT
/INSTALL=UPDATER	Enables the AutoUpdate 7.0 component if it has already been installed, and does NOT change whether the agent is enabled. This command-line option upgrades the agent. Sample: FRAMEPKG /NSTALL=UPDATER
/INSTDIR	Specifies the installation folder on the desired system. You can use Windows system variables, such as <SYSTEM_DRIVE>. If not specified, the default location is:<DRIVE>:\program files\mcafee\common framework Sample: FRAMEPKG /INSTALL=AGENT /INSTDIR=C:\ePOAgent
/REMOVE=AGENT	Disables the agent, and removes it if not in use. Sample: FRMINST /REMOVE=AGENT
/SILENT or /S	Installs the agent in silent mode, hiding the installation interface from the end-user. Sample: FRAMEPKG /INSTALL=AGENT /SILENT
/SITEINFO	Specifies the folder path to a specific repository list (SITELIST.XML) file. Sample: FRAMEPKG /INSTALL=AGENT /SITEINFO=C:\MYSITELIST.XML
/USELANGUAGE	Specifies the language version of the agent that you want to install. If you select a locale other than the 12 languages with locale IDs, the software appears in English. If you install multiple language versions, the locale selected in operating system determines the language version that displays. Sample: FRAMEPKG /INSTALL=AGENT /USELANGUAGE 0404

Creating Repositories

Security software is only as effective as the latest installed updates. For example, if your DAT files are out-of-date, even the best anti-virus software cannot detect new threats. It is critical that you develop a robust updating strategy to keep your security software as current as possible.

ePolicy Orchestrator software's repository architecture offers flexibility to ensure deploying and updating software is as easy and automated as your environment allows. Once your repository infrastructure is in place, create update tasks that determine how, where, and when your software is updated.

Are you creating repositories for the first time?

When creating and setting up repositories for the first time:

1. Understand the purpose of each type of repository, repository branch, and site.
2. Decide which types of repositories to use and their locations.
3. Create and populate your repositories.

Contents

- Repository types and what they do
- How repositories work together
- Ensuring access to the source site
- Working with source and fallback sites
- Using SuperAgents as distributed repositories
- Creating and configuring FTP, HTTP, and UNC repositories
- Working with the repository list files
- Changing credentials on multiple distributed repositories

Repository types and what they do

To deliver products and updates throughout your network, ePolicy Orchestrator offers several types of repositories that create a robust update infrastructure when used together. These provide the flexibility to develop an updating strategy to ensure your systems stay up-to-date.

Master repository

The master repository maintains the latest versions of security software and updates for your environment. This repository is the source for the rest of your environment. There is one master repository for each ePolicy Orchestrator server.

The master repository is configured when installed. However, you must ensure that proxy server settings are configured correctly. By default, ePolicy Orchestrator uses Microsoft Internet Explorer proxy settings.

Distributed repositories

Distributed repositories host copies of your master repository's contents. Consider using distributed repositories and placing them throughout your network strategically to ensure managed systems are updated while network traffic is minimized, especially across slow connections.

As you update your master repository, ePolicy Orchestrator replicates the contents to the distributed repositories.

Replication can occur:

- Automatically when specified package types are checked in to the master repository with global updating.
- On a recurring schedule with Replication tasks.
- Manually, by running a Replicate Now task.

A large organization can have multiple locations with limited bandwidth connections between them. Distributed repositories help reduce updating traffic across low-bandwidth connections. If you create a distributed repository in the remote location and configure the systems within the remote location to update from this distributed repository, the updates are copied across the slow connection only once — to the distributed repository — instead of once to each system in the remote location.

If global updating is enabled, distributed repositories update managed systems automatically, as soon as selected updates and packages are checked into the master repository. You do not need to spend additional time creating and configuring repositories or the update tasks.

Source site

The source site provides all updates for your master repository. The default source site is the McAfeeHttp update site, but you can change the source site or create multiple source sites if you require. McAfee recommends using the McAfeeHttp or McAfeeFtp update sites as your source site.

NOTE: Source sites are not required. You can download updates manually and check them in to your master repository. However, using a source site automates this process.

McAfee posts software updates to these sites regularly. For example, DAT files are posted daily. Update your master repository with updates as they are available.

Use pull tasks to copy source site contents to the master repository.

The McAfee update sites provide detection definition (DAT) and scanning engine file updates, as well as some language packs. You must check in all other packages and updates to the master repository manually.

Fallback site

The fallback site is a source site that's been enabled as the fallback, from which managed systems can retrieve updates when their usual repositories are inaccessible. For example, when network outages or virus outbreaks occur, accessing the established location may be difficult. Therefore, managed systems can remain up-to-date in such situations. The default fallback site is the McAfee HTTP (McAfeeHttp) update site. You can enable only one fallback site.

If managed systems use a proxy server to access the Internet, you must configure agent policy settings for those systems to use proxy servers when accessing this fallback site.

Types of distributed repositories

ePolicy Orchestrator supports four types of distributed repositories. Consider your environment and needs when determining which type of distributed repository to use. You are not limited to using one type, and may need several, depending on your network.

SuperAgent repositories

Use systems hosting SuperAgents as distributed repositories. SuperAgent repositories have several advantages over other types of distributed repositories:

- Folder locations are created automatically on the host system before adding the repository to the repository list.
- File sharing is enabled automatically on the SuperAgent repository folder.
- SuperAgent repositories don't require additional replication or updating credentials — its account permissions are created when the agent is converted to a SuperAgent.

  TIP: Although SuperAgent broadcast wake-up call functionality requires a SuperAgent in each broadcast segment, this is not a requirement for SuperAgent repository functionality. Managed systems only need to "see" the system hosting the repository.

- SuperAgents and global updating use a proprietary network protocol, SPIPE.

  TIP: McAfee recommends combining SuperAgent repositories and global updating to ensure your managed environment is up-to-date.

FTP repositories

If you are unable to use SuperAgent repositories, use an existing FTP server to host a distributed repository. Use your existing FTP server software such as Microsoft Internet Information Services (IIS) to create a new folder and site location for the distributed repository. See your web server documentation for details.

HTTP repositories

If you are unable to use SuperAgent repositories, use an existing HTTP server to host a distributed repository. Use your existing HTTP server software such as Microsoft Internet Information Services (IIS) to create a new folder and site location for the distributed repository. See your web server documentation for details.

UNC share repositories

If you are unable to use SuperAgent repositories, create a UNC shared folder to host a distributed repository on an existing server. Be sure to enable sharing across the network for the folder so that the ePolicy Orchestrator server can copy files to it and agents can access it for updates.

Unmanaged repositories

If you are unable to use managed distributed repositories, ePolicy Orchestrator administrators can create and maintain distributed repositories that are not managed by ePolicy Orchestrator.

If a distributed repository is not managed, a local administrator must keep it up-to-date manually.

Once the distributed repository is created, use ePolicy Orchestrator to configure managed systems of a specific System Tree group to update from it.

TIP: McAfee recommends that you manage all distributed repositories through ePolicy Orchestrator. This and using global updating, or scheduled replication tasks frequently, ensures your managed environment is up-to-date. Use unmanaged distributed repositories only if your network or organizational policy do not allow managed distributed repositories.

Repository branches and their purposes

ePolicy Orchestrator provides three repository branches, allowing you to maintain three versions of all packages in your master and distributed repositories. The repository branches are Current, Previous, and Evaluation. By default, ePolicy Orchestrator uses only the Current branch. You can specify branches when adding packages to your master repository. You can also specify branches when running or scheduling update and deployment tasks to distribute different versions to different parts of your network.

Update tasks can retrieve updates from any branch of the repository, but deployment tasks use the Current branch only.

To use the Evaluation and Previous branches for packages other than updates, you must select this in the Repository Packages server settings. Agent versions 3.6 and earlier can only retrieve update packages from the Evaluation and Previous branches.

Current branch

The Current branch is the main repository branch for the latest packages and updates. Product deployment packages can be added only to the Current branch, unless support for the other branches has been enabled.

Evaluation branch

You may want to test new DAT and engine updates with a small number of network segments or systems before deploying them to your entire organization. Specify the Evaluation branch when checking in new DATs and engines to the master repository, then deploy them to a small number of test systems. After monitoring the test systems for several hours, you can add the new DATs to your Current branch and deploy them to your entire organization.

Previous branch

Use the Previous branch to save and store the prior DAT and engine files before adding the new ones to the Current branch. In the event that you experience an issue with new DAT or engine files in your environment, you have a copy of previous versions that you can re-deploy to your systems if necessary. ePolicy Orchestrator saves only the most immediate previous version of each file type.

You can populate the Previous branch by selecting **Move existing packages to Previous branch** when you add new files to your master repository. The option is available when you pull updates from a source site and when you manually check in packages to the Current branch.

Repository list file and its uses

The repository list (SITELIST.XML) file contains the names of all the repositories you are managing. The repository list includes the location and encrypted network credentials that managed systems use to select the repository and retrieve updates. The server sends the repository list to the agent during agent-server communication.

If needed, you can export the repository list to external files (SITELIST.XML or SITEMGR.XML).

Use an exported SITELIST.XML file to:

- Import to an agent at installation.
- Import the repository list from a previous installation of ePolicy Orchestrator or from another McAfee product.

Use an exported SITEMGR.XML file to:

- Back up and restore your distriubted repositories and source sites if you need to reinstall the server.
- Import the distributed repositories and source sites from a previous installation of ePolicy Orchestrator.

How repositories work together

The repositories work together in your environment to deliver updates and software to managed systems. You may or may not need distributed repositories.

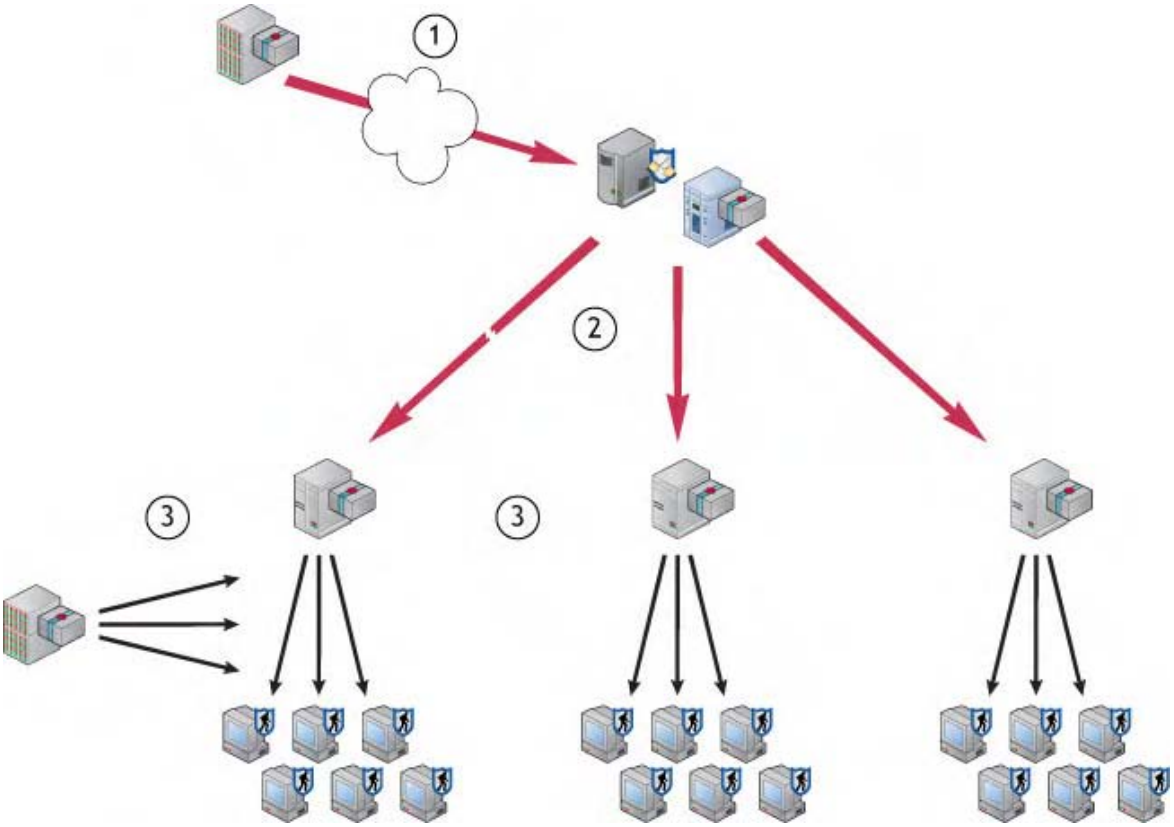

Figure 18: Sites and Repositories Delivering Packages to Systems

1 The master repository regularly pulls DAT and engine update files from the source site.

2 The master repository replicates the packages to distributed repositories in the network.

3 The managed systems in the network retrieve updates from a close repository. If managed systems can't access the distributed repositories or the master repository, they retrieve updates from the fallback site.

Ensuring access to the source site

Use these tasks to ensure the master repository and managed systems can access the Internet when using the McAfeeHttp and the McAfeeFtp sites as source and fallback sites. McAfee recommends using the Internet Explorer proxy server settings.

You can also configure proxy server settings from the console. You may need to do this if you cannot use the proxy settings in your Internet Explorer browser or if you do not use a proxy server.

Tasks

- Using Internet Explorer proxy settings for the master repository
- Configuring custom proxy settings for the master repository

Using Internet Explorer proxy settings for the master repository

Use these tasks to configure both Internet Explorer and ePolicy Orchestrator to use Internet Explorer proxy settings. If a source site must be accessed via the Internet, such as the McAfee update sites, the master repository uses proxy settings to retrieve packages. If your organization uses proxy servers to connect to the Internet, you must use the proxy server.

By default, ePO is configured to use the proxy settings for the Internet Explorer browser that is installed on your ePO server.

NOTE: A user must be logged on to the ePO server sytem for the scheduled tasks to run when using Internet Explorer proxy settings. If you do not want to leave an account logged on to the server (even if locked), you must manually enter proxy authentication information.

Tasks

- Configuring Internet Explorer proxy settings
- Configuring ePolicy Orchestrator to use Internet Explorer proxy settings

Configuring Internet Explorer proxy settings

Use this task to configure LAN and proxy settings within Internet Explorer if you cannot access the Internet from the server system.

Before you begin

Before using this task, you can confirm that these Internet Explorer settings are configured correctly. Launch Internet Explorer on the server and browse to www.mcafee.com. If you can access this site your proxy settings are correct.

Task

1. Launch Internet Explorer.
2. Select **Tools** | **Internet Options** from the menu bar.
3. Select the **Connections** tab, then select **LAN Settings** at the bottom of the dialog box.
4. In the **LAN Settings** dialog box, select **Use a proxy server for your LAN**.
5. Click **Advanced**. The **Proxy Settings** dialog box appears.

6 Type proxy information into the appropriate fields. To use the default source and fallback sites, enter the information for HTTP and FTP.

7 Select **Use the same proxy for all protocols** so both FTP and HTTP correctly use the proxy.

8 Click **OK** to close the **Proxy Settings** dialog box.

9 Select **Bypass proxy for local addresses** options.

10 Click **OK** to close the **LAN Settings** dialog box.

11 Click **OK** to close the **Internet Options** dialog box.

Configuring ePolicy Orchestrator to use Internet Explorer proxy settings

Use this task to configure ePolicy Orchestrator to use Internet Explorer's proxy settings. This is the default setting.

Task

For option definitions, click **?** on the page displaying the options.

1 Go to **Software | Master Repository**, then click **Configure Proxy Settings**. The **Configure Proxy Settings** page appears.

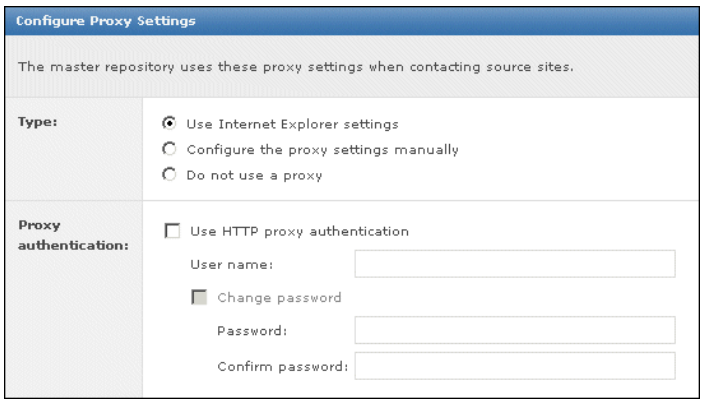

Figure 19: Configure Proxy Settings page

2 Ensure **Use Internet Explorer settings** is selected next to **Type**.

3 Click **OK**.

Configuring custom proxy settings for the master repository

Use this task if you must use custom proxy settings for the master repository. If you cannot allow ePolicy Orchestrator to use the proxy settings in your Internet Explorer browser, or if you do not use a proxy server, you must configure the proxy settings or select to not use proxy settings.

Task

For option definitions, click **?** on the page displaying the options.

1 Go to **Software | Master Repository**, then click **Configure Proxy Settings**. The **Configure Proxy Settings** page appears.

2 Select **Configure the proxy settings manually**.

If your server does not need a proxy to access the Internet, select **Don't use proxy settings**, then click **OK**.

3 Next to **Proxy authentication**, configure the settings as appropriate, depending on whether you pull updates from HTTP repositories, FTP repositories, or both.

4 Next to **Proxy server**, select whether to use one proxy server for all communication, or different proxy servers for HTTP and FTP proxy servers. Then type the **Address** (IP address or fully-qualified domain name) and the **Port** number of the proxy server.

NOTE: If you are using the default source and fallback sites, or if you configure another HTTP source site and FTP fallback site (or vice versa), configure both HTTP and FTP proxy authentication information here.

5 Next to **Exclusions**, select **Bypass Local Addresses** then specify any distributed repositories to which the server can connect directly by typing the IP addresses or fully-qualified domain name of those systems separated by semi-colons.

6 Click **OK** to save these settings.

Working with source and fallback sites

Use these tasks to change the default source and fallback sites. You must be a global administrator to define, change, or delete source or fallback sites. You can edit settings, delete existing source and fallback sites, or switch between them.

McAfee recommends using the default source and fallback sites. If you require different sites for this purpose, you can create new ones.

Tasks

- Switching source and fallback sites
- Creating source sites
- Editing source and fallback sites
- Deleting source or fallback sites

Switching source and fallback sites

Use this task to change which sites are the source and fallback sites. Depending on your network configuration, you may find that HTTP or FTP updating works better. Therefore, you may want to switch the source and fallback sites.

Before you begin

You must have appropriate permissions to perform this task.

Task

For option definitions, click **?** on the page displaying the options.

1 Go to **Software | Source sites**. A list of all sites that can be used as the source or fallback appear.

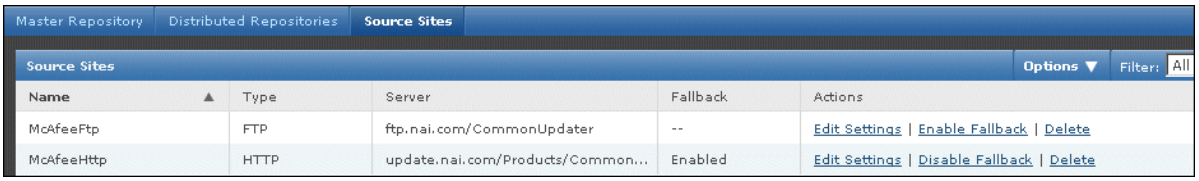

Figure 20: Source Sites tab

2 Locate the site in the list that you want to be the fallback, then click **Enable Fallback** next to it.

Creating source sites

Use this task to create a new source site.

Before you begin

You must have appropriate permissions to perform this task.

Task

For option definitions, click **?** on the page displaying the options.

1 Go to **Software | Source Sites**, then click **New Source Site**. The **Source Site Builder** wizard appears.

2 On the **Description** page, type a unique name and select **HTTP**, **UNC**, or **FTP**, then click **Next**.

3 On the **Server** page, provide the address and port information of the site, then click **Next**.

- If you selected **FTP**, type the web address in **URL** and the FTP port number in **Port**.
- If you selected **HTTP**, type the web address in **URL** and the HTTP port number in **Port**. (You can also enter the server name or IP address in the **URL** text box.)
- If you selected **UNC**, type the network directory where the site resides in **Replication UNC path**. Use this format: \\<computer>\<FOLDER>. You can use variables to define this location.

4 On the **Credentials** page, provide the download credentials used by managed systems to connect to this repository, then click **Next**. Use credentials with read-only permissions to the HTTP server, FTP server, or UNC share that hosts the site.

- If you selected **FTP**, select **Anonymous** or **FTP authentication** (if the server requires authentication) then type the user account information in **User name**, **Password**, and **Confirm password**.
- If you selected **HTTP**, select **Anonymous** or **HTTP authentication** (if the server requires authentication), then type the user account information in **User name**, **Password**, and **Confirm password**.
- If you selected **UNC**, type the user account information in **Domain**, **User name**, **Password**, and **Confirm password**.

To test the user account you specified, click **Test Credentials**.

5 Click **Next**. The **Summary** page appears.

6 Click **Save** to add the site to the list.

Editing source and fallback sites

Use this task to edit the settings of source or fallback sites, such as URL address, port number, and download authentication credentials.

Before you begin

You must have appropriate permissions to perform this task.

Task

For option definitions, click **?** on the page displaying the options.

1 Go to **Software | Source Sites**. A list of all sites that can be used as the source or fallback appears.

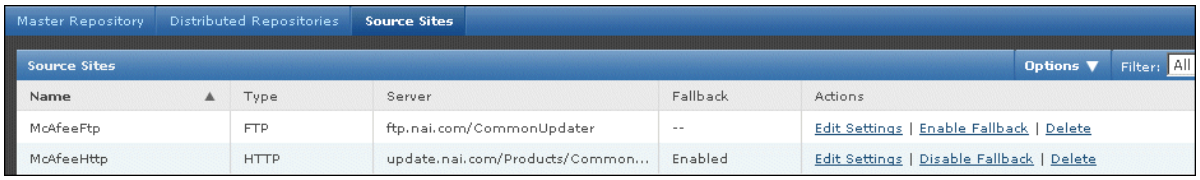

Figure 21: Source Sites tab

2 Locate the site in the list, then click **Edit Settings** next to it. The **Source Site Builder** wizard appears.

3 Edit the settings on the wizard pages as needed, then click **Save**.

Deleting source or fallback sites

Use this task to delete source or fallback sites.

Before you begin

You must have appropriate permissions to perform this task.

Task

For option definitions, click **?** on the page displaying the options.

1 Go to **Software | Source Sites**, then click **Delete** next to the site. The **Delete Source Site** dialog box appears.

2 Click **OK**.

The site is removed from the **Source Sites** page.

Using SuperAgents as distributed repositories

Use these tasks to create and configure repositories on systems hosting SuperAgents. You cannot create these until agents have been distributed to the desired systems.

Tasks

- Creating SuperAgent repositories
- Selecting which packages are replicated to SuperAgent repositories

▸ Deleting SuperAgent distributed repositories

Creating SuperAgent repositories

Use this task to create a SuperAgent repository. The desired system must have an ePO agent installed and running. McAfee recommends using SuperAgent repositories with global updating.

This task assumes that you know where the desired systems are located in the System Tree. McAfee recommends that you create a "SuperAgent" tag so that you can easily locate the systems with the **Tag Catalog** page, or by running a query.

Task

For option definitions, click **?** on the page displaying the options.

1. Go to **Systems | Policy Catalog**, then select **McAfee Agent** from the **Product** drop-down list, then select **General** from the **Category** drop-down list.
2. Create a new policy, duplicate an existing one, or open one that's already applied to systems hosting a SuperAgent that you want to host SuperAgent repositories.
3. Select the **General** tab, then ensure **Convert agents to SuperAgents** is selected.
4. Select **Use systems running SuperAgents as distributed repositories**, then type a folder path location for the repository. This is the location to which the master repository copies updates during replication. You can use standard Windows variables, such as <PROGRAM_FILES_DIR>.

   NOTE: Managed systems updating from this SuperAgent repository are able to access this folder. You do not need to manually enable file sharing.

5. Click **Save**.
6. Assign this policy to each system you want to host a SuperAgent repository.

The next time the agent calls in to the server, the new configuration is retrieved. When the distributed repository is created, the folder you specified is created on the system if it did not already exist. If the folder you specify cannot be created, one of two folders is created:

- <DOCUMENTS AND SETTINGS>\ ALL USERS\APPLICATION DATA\MCAFEE\FRAMEWORK\DB\SOFTWARE
- <AGENT INSTALLATION PATH>\DATA\DB\SOFTWARE

In addition, the location is added to the repository list (SITELIST.XML) file. This makes the site available for updating by systems throughout your managed environment.

If you do not want to wait for the next agent-server communication, you can send an agent wake-up call to the desired systems.

Selecting which packages are replicated to SuperAgent repositories

Use this task to select which repository-specific packages are replicated to any distributed repository.

Task

For option definitions, click **?** on the page displaying the options.

1 Go to **Software | Distributed Repositories**. A list of all distributed repositories appears.
2 Locate the desired SuperAgent repository, then click **Edit Package Types** under **Actions**.
3 Select package types as needed.

   NOTE: Ensure that all packages required by any managed system using this repository are selected. Managed systems go to one repository for all packages — the task fails for systems that are expecting to find a package type that is not present. This feature ensures packages that are used only by a few systems are not replicated throughout your entire environment.

4 Click **Save**.

Deleting SuperAgent distributed repositories

Use the task to remove SuperAgent distributed repositories from the host system and the repository list (SITELIST.XML). New configurations take effect during the next agent-server communication.

Task

For option definitions, click **?** on the page displaying the options.

1 Open the desired McAfee Agent policy pages (in edit mode) from the desired assignment point in the System Tree or from the **Policy Catalog** page.
2 On the **General** tab, deselect **Use systems running SuperAgents as distributed repositories**, then click **Save**.

   NOTE: To delete a limited number of your existing SuperAgent distributed repositories, duplicate the McAfee Agent policy assigned to these systems and deselect **Use systems running SuperAgents as distributed repositories** before saving it. Assign this new policy as needed.

The SuperAgent repository is deleted and removed from the repository list. However, the agent still functions as a SuperAgent as long as you leave the **Convert agents to SuperAgents** option selected.

Creating and configuring FTP, HTTP, and UNC repositories

Use these tasks to host distributed repositories on existing FTP, HTTP servers or UNC shares. Although you do not need to use a dedicated server, the system should be powerful enough for the desired number of managed systems to connect for updates.

Tasks

- Creating a folder location on an FTP, HTTP server or UNC share
- Adding the distributed repository to ePolicy Orchestrator
- Enabling folder sharing for UNC and HTTP repositories
- Editing distributed repositories
- Deleting distributed repositories

Creating a folder location on an FTP, HTTP server or UNC share

Use this task to create the folder that hosts repository contents on the distributed repository system:

Task

- For UNC share repositories, create the folder on the system and enable sharing.
- For FTP or HTTP repositories, use your existing FTP or HTTP server software, such as Microsoft Internet Information Services (IIS), to create a new folder and site location. See your web server documentation for details.

Adding the distributed repository to ePolicy Orchestrator

Use this task to add the new distributed repository to the repository list and configure it to use the folder you created.

Task

For option definitions, click **?** on the page displaying the options.

1. Go to **Software | Distributed Repositories**, then click **New Repository**. The **Distributed Repository Builder** wizard appears.
2. On the **Description** page, type a unique name and select **HTTP**, **UNC**, or **FTP**, then click **Next**. This is the name that appears in the repository list. The name does not need to be the name of the system hosting the repository.
3. On the **Server** page, provide the address and port information of the repository, then click **Next**:
   - If you selected **FTP**, type the web address in **URL** and the FTP port number in **Port**, which is **21** by default.
   - If you selected **HTTP**, type the web address in **URL** and the HTTP port number in **Port**, which is **80** by default, and type the network directory where the repository resided in **Replication UNC path**. (You can also enter the server name or IP address in the **URL** text box.)
   - If you selected **UNC**, type the network directory where the repository resides in **Replication UNC path**. Use this format: \\<COMPUTER>\<FOLDER>. You can use variables to define this location.
4. On the **Credentials** page, provide the **Download credentials** used by managed systems to connect to this repository, then click **Next**. Use credentials with read-only permissions to the HTTP server, FTP server, or UNC share that hosts the repository:
   - If you selected **FTP**, select **Anonymous** or **FTP authentication** (if the server requires authentication) then type the user account information in **User name**, **Password**, and **Confirm password**.
   - If you selected **HTTP**, select **Anonymous** or **HTTP authentication** (if the server requires authentication), then type the user account information in **User name**, **Password**, and **Confirm password**.
   - If you selected **UNC**, whether to use the credentials of the logged-on account, or type user account information in **Domain**, **User name**, **Password**, and **Confirm password**.
5. Click **Test Credentials**. After a few seconds, a confirmation message appears that the site is accessible to systems using the authentication information.

If credentials are incorrect, check the:

- User name and password.
- URL or path on the previous panel of the wizard.
- The HTTP, FTP or UNC site on the system.

6 Enter **Replication credentials**. The server uses these credentials when it replicates DAT files, engine files, or other product updates from the master repository to the distributed repository. These credentials must have both read and write permissions for the distributed repository:

- If you selected **FTP**, type the user account information in **User name**, **Password**, and **Confirm password**.
- If you selected **HTTP** and the HTTP server requires authentication, type the user account information in **Domain**, **User name**, and **Password** fields.
- If you selected **UNC**, type the user account information for the network directory in **Domain**, **User name**, **Password**, and **Confirm password**.

7 Click **Test Credentials**. After a few seconds, a confirmation message appears that the site is accessible to systems using the authentication information.

8 Click **Next**. The **Package Types** page appears.

9 Select whether to replicate all packages or selected packages to this distributed repository, then click **Next**.

NOTE: Ensure all packages required by managed systems using this repository are not deselected. Managed systems go to one repository for all packages — if a needed package type is not present in the repository, the task fails. This feature ensures packages that are only used by a few systems are not replicated throughout your entire environment.

10 Click **Save** to add the repository. ePolicy Orchestrator adds the new distributed repository to its database.

Enabling folder sharing for UNC and HTTP repositories

Use this task to share a folder on an HTTP or UNC distributed repository. For these repositories, ePolicy Orchestrator requires that the folder is enabled for sharing across the network so that your ePolicy Orchestrator server can copy files to it. This is for replication purposes only. Managed systems configured to use the distributed repository use the appropriate protocol (HTTP, FTP, or Windows file sharing) and do not require folder sharing.

Task

1 On the system, locate the folder you created using Windows Explorer.

2 Right-click the folder, then select **Sharing**.

3 On the **Sharing** tab, select **Share this folder**.

4 Configure share permissions as needed. Systems updating from the repository require only read access, but administrator accounts, including the account used by the ePolicy Orchestrator server service, require write access. See your Microsoft Windows documentation to configure appropriate security settings for shared folders.

5 Click **OK**.

Editing distributed repositories

Use this task to edit a distributed repository.

Task

For option definitions, click **?** on the page displaying the options.

1. Go to **Software | Distributed Repositories**, then select **Edit Settings** next to the desired repository. The **Distributed Repository Builder** wizard opens with the details of the distributed repository.
2. Change configuration, authentication, and package selection options as needed.
3. Click **Save**.

Deleting distributed repositories

Use this task to delete HTTP, FTP, or UNC distributed repositories. Doing this removes them from the repository list and removes the distributed repository contents.

Before you begin

You must have appropriate permissions to perform this task.

Task

For option definitions, click **?** on the page displaying the options.

1. Go to **Software | Distributed Repositories**, then click **Delete** next to the desired repository.
2. On the **Delete Repository** dialog box, click **OK**.

   NOTE: Deleting the repository does not delete the packages on the system hosting the repository.

Working with the repository list files

Use these tasks to export the SITELIST.XML file for use by the agent and supported products, or the SITEMGR.XML file for use when reinstalling the ePO server or for import into other ePO servers that you want to use the same distributed repositories or source sites.

Tasks

- Exporting the repository list SITELIST.XML file
- Exporting the repository list SITEMGR.XML file for backup or use by other servers
- Importing distributed repositories from the SITEMGR.XML file
- Importing source sites from the SITEMGR.XML file

Exporting the repository list SITELIST.XML file

Use this task to export the repository list (SITELIST.XML) file to a file for manual delivery to systems, or for import during the installation of supported products.

Before you begin

You must have appropriate permissions to perform this task.

Task

For option definitions, click **?** on the page displaying the options.

1. Go to **Software | Master Repository**, then click **Export Sitelist**. The **File Download** dialog box appears.
2. Click **Save**. The **Save As** dialog box appears.
3. Browse to the location to save the SITELIST.XML file, then click **Save**.

Once you have exported this file, you can import it during the installation of supported products. For instructions, see the installation guide for that product.

You can also distribute the repository list to managed systems, then apply the repository list to the agent.

Exporting the repository list SITEMGR.XML file for backup or use by other servers

Use this task to export the list of distributed repositories and source sites as the SITEMGR.XML file. Use this file to restore the distributed repositories and source sites when you reinstall the ePO server, or when you want to share distributed repositories or source sites with another ePO server.

You can export this file from either the **Distributed Repositories** or **Source Sites** pages. However, when you import this file to either page, it imports only the items from the file that are listed on that page. For example, when this file is imported to the **Distributed Repositories** page, only the distributed repositories in the file are imported. Therefore, if you want to import both distributed repositories and source sites, you must import the file twice, once from each page.

Before you begin

You must have appropriate permissions to perform this task.

Task

For option definitions, click **?** on the page displaying the options.

1. Go to **Software | Distributed Repositories** (or **Software | Source Sites**), then click **Export Repositories** (or **Export Source Sites**). The **File Download** dialog box appears.
2. Click **Save**, then browse to and select the location to save the file.
3. Rename the file if needed, then click **Save**.

Importing distributed repositories from the SITEMGR.XML file

Use this task to import distributed repositories from a repository list file. This is valuable after reinstalling a server, or if you want one server to use the same distributed repositories as another server.

Before you begin

You must have appropriate permissions to perform this task.

Task

For option definitions, click **?** on the page displaying the options.

1 Go to **Software | Distributed Repositories**, then click **Import Repositories**. The **Import Repositories** dialog box appears.

2 Browse to and select the exported SITEMGR.XML file. The **Import Repositories** page appears.

3 Select the desired distributed repositories to import into this server, then click **OK**.

The selected repositories are added to the list of repositories on this server.

Importing source sites from the SITEMGR.XML file

Use this task to import source sites from a repository list file. This is valuable after reinstalling a server, or if you want one server to use the same distributed repositories as another server.

Before you begin

You must have appropriate permissions to perform this task.

Task

For option definitions, click **?** on the page displaying the options.

1 Go to **Software | Source Sites**, then click **Import Source Sites**. The **Import Source Sites** dialog box appears.

2 Browse to and select the exported SITEMGR.XML file. The **Import Source Sites** page appears.

3 Select the desired source sites to import into this server, then click **OK**.

The selected source sites are added to the list of repositories on this server.

Changing credentials on multiple distributed repositories

Use this task to change credentials on multiple distributed repositories of the same type. This task is valuable in environments where there are many distributed repositories.

Before you begin

You must have appropriate permissions to perform this task.

Task

For option definitions, click **?** on the page displaying the options.

1 Go to **Software | Distributed Repositories**, then click **Change Credentials**. The **Repository Type** page of the **Change Credentials** wizard appears.

2 Select the type of distributed repository for which you want to change credentials, then click **Next**. The **Repository Selection** page appears.

3 Select the desired distributed repositories, then click **Next**. The **Credentials** page appears.

4 Edit the credentials as needed, then click **Next**. The **Summary** page appears.

5 Review the information, then click **Save**.

Managing Products with Policies and Client Tasks

Managing products from a single location is a central feature of ePolicy Orchestrator and is accomplished through the combination of product policies and client tasks. Policies ensure a product's features are configured correctly, while client tasks are the scheduled actions that run on the managed systems hosting any client-side software.

Are you configuring policies and tasks for the first time?

When configuring policies and tasks for the first time:

1. Understand product management in ePolicy Orchestrator.
2. Plan product policies and client tasks for the segments of your System Tree.
3. Create and assign policies to groups and systems.
4. Create and assign client tasks to groups and systems.

Contents

- Extensions and what they do
- Policy management
- Policy application
- Client tasks and what they do
- Bringing products under management
- Viewing policy information
- Working with the Policy Catalog
- Working with policies
- Working with client tasks
- Frequently asked questions

Extensions and what they do

Extensions are ZIP files you install on the ePO server in order to manage another security product in your environment. The extensions contain the files, components, and information necessary to manage such a product. Extensions replace the NAP files of previous releases.

What functionality extensions add

When a managed product extension is installed, functionalities added can include:

- Policy pages.
- Server tasks.
- Client tasks.
- Default queries.
- New result types, chart types, and properties to select with the Query Builder wizard.
- Default Dashboards and dashboard monitors.
- Feature permissions that can be assigned to user accounts.
- Additional product-specific functionalities.

Where extension files are located

Some extensions are installed automatically when ePolicy Orchestrator is installed. For products whose extensions are not installed by default, see the product documentation for the name and its location on the product CD or in the product download.

Policy management

A policy is a collection of settings that you create, configure, then enforce. Policies ensure that the managed security software products are configured and perform accordingly. For example, if end users disable anti-virus scans, you can set a policy that re-enables the scan at the policy enforcement interval (five minutes by default).

Some policy settings are the same as the settings you configure in the interface of the product installed on the managed system. Other policy settings are the primary interface for configuring the product or component. The ePolicy Orchestrator console allows you to configure policy settings for all products and systems from a central location.

Policy categories

Policy settings for most products are grouped by category. Each policy category refers to a specific subset of policy settings. Policies are created by category. In the **Policy Catalog** page, policies are displayed by product and category. When you open an existing policy or create a new policy, the policy settings are organized across tabs.

Where policies are displayed

To see all of the policies that have been created per policy category, go to the **Systems | Policy Catalog** page, then select the desired **Product** and **Category** from the drop-down lists. On the **Policy Catalog** page, users can see only policies of the products to which they have permissions.

To see which policies, per product, are applied to a specific group of the System Tree, go to the **Systems | System Tree | Policies** page, select the desired group, then select the desired **Product** from the drop-down list.

NOTE: A McAfee Default policy exists for each category. You cannot delete, edit, export or rename these policies, but you are not required to assign the McAfee Default policies to any groups or systems.

Setting policy enforcement

For each managed product or component, choose whether the agent enforces all or none of its policy selections for that product or component.

From the **Policies** page, choose whether to enforce policies for products or components on the selected group.

In the **Policy Catalog** page, you can view assignments, per policy, where the it is applied but not enforced.

When policies are enforced

When you reconfigure policy settings, the new settings are delivered to, and enforced on, the managed systems at the next agent-server communication. The frequency of this communication is determined by the **Agent-to-server-communication interval** settings on the **General** tab of the **McAfee Agent**policy pages, or the Agent Wakeup task schedule (depending on how you implement agent-server communication). This interval is set to occur once every 60 minutes by default.

Once the policy settings are in effect on the managed system, the agent continues to enforce policy settings locally at a regular interval. This enforcement interval is determined by the **Policy enforcement interval** setting on the **General** tab of the **McAfee Agent**policy pages. This interval is set to occur every five minutes by default.

Policy settings for McAfee products are enforced immediately at the policy enforcement interval and at each agent-server communication if policy settings have changed.

NOTE: There is a delay of up to three minutes after the interval before policies for Norton AntiVirus products are enforced. The agent first updates the GRC.DAT file with policy information, then the Norton AntiVirus product reads the policy information from the GRC.DAT file, which occurs approximately every three minutes.

Exporting and importing policies

If you have multiple servers, you can export and import policies between them via XML files. In such an environment, you only need to create a policy once.

You can export and import individual policies, or all policies for a given product.

This feature can also be used to back up policies if you need to re-install the server.

Policy application

Policies are applied to any system by one of two methods, inheritance or assignment.

Inheritance

Inheritance determines whether the policy settings and client tasks for a group or system are taken from its parent. By default, inheritance is enabled throughout the System Tree.

When you break this inheritance by assigning a new policy anywhere in the System Tree, all child groups and systems that are set to inherit the policy from this assignment point do so.

Assignment

You can assign any policy in the Policy Catalog to any group or system (provided you have the appropriate permissions). Assignment allows you to define policy settings once for a specific need, then apply the policy to multiple locations.

When you assign a new policy to a particular group of the System Tree, all child groups and systems that are set to inherit the policy from this assignment point do so.

Assignment locking

You can lock the assignment of a policy on any group or system (provided you have the appropriate permissions). Assignment locking prevents other users:

- With appropriate permissions at the same level of the System Tree from inadvertently replacing a policy.
- With lesser permissions (or the same permissions but at a lower level of the System Tree) from replacing the policy.

Assignment locking is inherited with the policy settings.

Assignment locking is valuable when you want to assign a certain policy at the top of the System Tree and ensure no other users replace it anywhere in the System Tree.

Assignment locking only locks the assignment of the policy, but does not prevent the policy owner from making changes to its settings. Therefore, if you intend to lock a policy assignment, ensure that you are the owner of the policy.

Policy ownership

All policies for products and features to which you have permissions are available from the **Policy Catalog** page. To prevent any user from editing other users' named policies, each policy is assigned an owner — the user who created it.

Ownership provides that no one can modify or delete a policy except its creator or a global administrator. Any user (with appropriate permissions) can assign any policy in the **Policy Catalog** page, but only the owner or a global administrator can edit it.

If you assign a policy that you do not own to managed systems, be aware that if the owner of the named policy modifies it, all systems where this policy is assigned receive these modifications.

Therefore, if you wish to use a policy owned by a different user, McAfee recommends that you first duplicate the policy, then assign the duplicate to the desired locations. This provides you ownership of the assigned policy.

Client tasks and what they do

ePolicy Orchestrator allows you to create and schedule client tasks that run on managed systems.

You can define tasks for the entire System Tree, a specific group, or an individual system. Like policy settings, client tasks are inherited from parent groups in the System Tree.

Which extension files are installed on your ePO server determines which client tasks are available.

Client tasks are commonly used for:

- Product deployment.
- Product functionality. (For example, the VirusScan Enterprise On-Demand Scan task.)
- Upgrades and updates.

See the product documentation for your managed products for information and instructions.

Bringing products under management

Use this task to install an extension (ZIP) file. A product's extension must be installed before ePolicy Orchestrator can manage the product.

Before you begin

You must have appropriate permissions to perform this task.

Task

For option definitions, click **?** on the page displaying the options.

1. Ensure the extension file is in accessible location on the network.
2. Go to **Configuration | Extensions**, then click **Install Extension**. The **Install Extension** dialog box appears.
3. Browse to and select the desired extension (ZIP) file, then click **OK**.
4. Verify the product name appears in the **Extensions** list.

Viewing policy information

Use these tasks to view detailed information about the policies, their assignments, inheritance, and their owners.

Tasks

- Viewing groups and systems where a policy is assigned
- Viewing the settings of a policy
- Viewing policy ownership
- Viewing assignments where policy enforcement is disabled
- Viewing policies assigned to a group
- Viewing policies assigned to a specific system
- Viewing a group's policy inheritance
- Viewing and resetting broken inheritance

Viewing groups and systems where a policy is assigned

Use this task to view the groups and systems where a policy is assigned. This list shows the assignment points only, not each group or system that inherits the policy.

Task

For option definitions, click **?** on the page displaying the options.

1 Go to **Systems | Policy Catalog**, then select the desired **Product** and **Category**. All created policies for that category appear in the details pane.

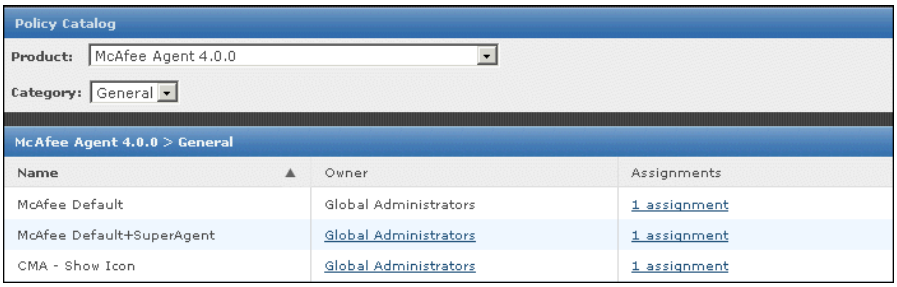

Figure 22: Policy Catalog page

2 Under **Assignments** on the row of the desired policy, click the blue text that indicates the number of groups or systems where the policy is assigned (for example, **6 assignments**).

On the **Assignments** page, each group or system where the policy is assigned appears with its **Node Name** and **Node Type**.

Viewing the settings of a policy

Use this task to view the specific settings of a policy.

Task

For option definitions, click **?** on the page displaying the options.

1 Go to **Systems | Policy Catalog**, then select the desired **Product** and **Category**. All created policies for the selected category are available in the details pane.

2 Click **Edit** next to the desired policy. The policy pages, and their settings appear.

NOTE: You can also view this information when accessing the assigned policies of a specific group, accessed from the **Systems | System Tree | Policies** page.

Viewing policy ownership

Use this task to view the owner of a policy.

Task

For option definitions, click **?** on the page displaying the options.

1 Go to **Systems | Policy Catalog**, then select the desired **Product** and **Category**. All created policies for the category appear in the details pane.

2 The owner of the policy is displayed under **Owner**.

Viewing assignments where policy enforcement is disabled

Use this task to view assignments where policy enforcement, per policy category, is disabled.

Task

For option definitions, click **?** on the page displaying the options.

1 Go to **Systems | Policy Catalog**, then select the desired **Product** and **Category**.

2 Click the blue text next to **Product enforcement status**, which indicates the number of assignments where enforcement is disabled, if any. The **Enforcement <policy name>** page appears.

3 Click any item in the list to go to its **Policies** page.

Viewing policies assigned to a group

Use this task to view the policies assigned to a group.

Task

For option definitions, click **?** on the page displaying the options.

1 Go to **Systems | System Tree | Policies**, then select the a group in the System Tree. All assigned policies, organized by product, appear in the details pane.

2 Click any policy to view its settings.

Viewing policies assigned to a specific system

Use this task to view the policies assigned to a specific system.

Task

For option definitions, click **?** on the page displaying the options.

1 Go to **Systems | System Tree | Systems**, then select the desired group in the System Tree. All systems belonging to the group appear in the details pane.

2 Select the system, then click **Modify Policies on a Single System**.

3 Select the product. The product's policies assigned to this system appear.

4 Click any policy to view its settings.

Viewing a group's policy inheritance

Use this task to view the policy inheritance of a specific group.

Task

For option definitions, click **?** on the page displaying the options.

1 Go to **Systems | System Tree | Policies**. All assigned policies, organized by product, appear in the details pane.

2 The desired policy row, under **Ineritance Source**, displays the name of the group from which the policy is inherited.

Viewing and resetting broken inheritance

Use this task to view where policy inheritance is broken.

Task

For option definitions, click **?** on the page displaying the options.

1 Go to **Systems | System Tree | Policies**. All assigned policies, organized by product, are appear in the details pane.

2 The desired policy row, under **Broken Inheritance**, displays the number of groups and systems where this policy's inheritance is broken.

NOTE: This is the number of groups or systems where the policy inheritance is broken, not the number of systems that do not inherit the policy. For example, if only one particular group does not inherit the policy, this is represented by **1 doesn't inherit**, regardless of the number of systems within the group.

3 Click the blue text indicating the number of child groups or systems that have broken inheritance. The **View broken inheritance** page displays a list of the names of these groups and systems.

4 To reset the inheritance of any of these, select the checkbox next to the name, then click **Reset Inheritance**.

Working with the Policy Catalog

Use these tasks to create and maintain policies from the Policy Catalog page.

Tasks

- Creating a policy on the Policy Catalog page
- Duplicating a policy on the Policy Catalog page
- Editing a policy's settings from the Policy Catalog
- Renaming a policy from the Policy Catalog
- Deleting a policy from the Policy Catalog

Creating a policy on the Policy Catalog page

Use this task to create a new policy on the Policy Catalog. Policies created here are by default not assigned to any groups or systems. When you create a policy here, you are adding a custom policy to the Policy Catalog.

You can create policies before or after a product is deployed.

Task

1 Go to **Systems | Policy Catalog**, then select the **Product** and **Category** from the drop-down lists. All created policies for that category appear in the details pane.

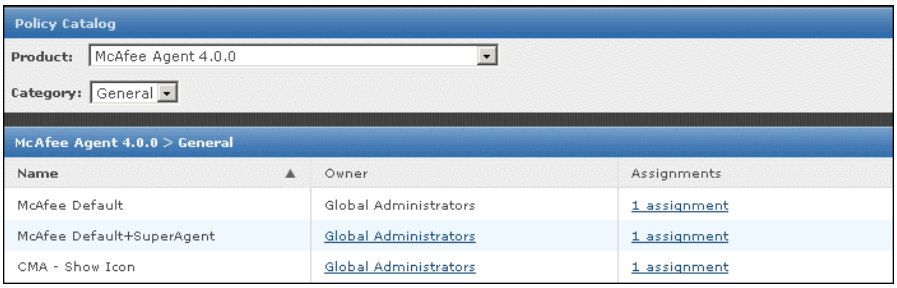

Figure 23: Policy Catalog page

2 Click **New Policy** at the bottom of the page. The **Create New Policy** dialog box appears.
3 Select the policy you want to duplicate from the **Create a policy based on this existing policy** drop-down list.
4 Type a name for the new policy in the **New policy name** field, then click **OK**. The **Policy Settings** dialog box appears for the new policy.
5 Edit the policy settings on each tab as needed.
6 Click **Save**.

Duplicating a policy on the Policy Catalog page

Use this task to create a new policy based on an existing one. For example, if you already have a policy that is similar to one you want to create, you can duplicate the existing one, then make the desired changes.

Task

For option definitions, click **?** on the page displaying the options.

1 Go to **Systems | Policy Catalog**, then select the **Product** and **Category** from the drop-down lists. All created policies for that category appear in the details pane.
2 Locate the policy to duplicate, then click **Duplicate** in that policy's row. The **Duplicate Existing Policy** dialog box appears.
3 Type the name of the new policy in the field, then click **OK** (for example, Sales Europe). The new policy appears on the **Policy Catalog** page.
4 Click **Edit** next to the new policy's name in the list. The policy settings appear.
5 Edit the settings as needed, then click **Save**.

Editing a policy's settings from the Policy Catalog

Use this task to modify the settings of a policy. Your user account must have appropriate permissions to edit policy settings for the desired product.

Task

For option definitions, click **?** on the page displaying the options.

1 Go to **Systems | Policy Catalog**, then select the **Product** and **Category** from the drop-down lists. All created policies for that category appear in the details pane.
2 Locate the desired policy, then click **Edit** next to it. The policy settings appear.
3 Edit the settings as needed, then click **Save**.

Renaming a policy from the Policy Catalog

Use this task to rename a policy. Your user account must have appropriate permissions to edit policy settings for the desired product.

Task

For option definitions, click **?** on the page displaying the options.

1 Go to **Systems | Policy Catalog**, then select the **Product** and **Category** from the drop-down lists. All created policies for that category appear in the details pane.
2 Locate the desired policy, then click **Rename** in the desired policy's row. The **Rename Policy** dialog box appears.
3 Type a new name for the existing policy, then click **OK**.

Deleting a policy from the Policy Catalog

Use this task to delete a policy from the Policy Catalog. When you delete a policy, all groups and systems where it is currently applied inherit the policy their parent group. Before deleting a policy, review the groups and systems where it is assigned, and assign a different policy if you don't want the group or system to inherit the policy from the parent group.

If you delete a policy that is applied to the My Organization group, the McAfee Default policy of this category is assigned.

Task

For option definitions, click **?** on the page displaying the options.

1 Go to **Systems | Policy Catalog**, then select the **Product** and **Category** from the drop-down lists. All created policies for that category appear in the details pane.
2 Locate the desired policy, then click **Delete** in the policy's row.
3 Click **OK** when prompted.

Working with policies

Use these tasks to assign and manage the policies in your environment.

Tasks

- Changing the owner of a policy
- Sharing policies between ePO servers
- Assigning a policy to a group of the System Tree
- Assigning a policy to a managed system
- Assigning a policy to multiple managed systems within a group
- Enforcing policies for a product on a group
- Enforcing policies for a product on a system
- Copying and pasting assignments

Changing the owner of a policy

Use this task to change the owner of a policy. By default, ownership is assigned to the user that created the policy.

Task

For option definitions, click **?** on the page displaying the options.

1 Go to **Systems | Policy Catalog**, then select the **Product** and **Category**. All created policies for that category appear in the details pane.
2 Locate the desired policy, then click the **Owner** of the policy. The **Assign Policy Owner** dialog box appears.
3 Select the desired owners of the policy from the list, then click **OK**.

Sharing policies between ePO servers

Use these tasks to share policies between servers. To do this, you must export the policy to an XML file from the **Policy Catalog** page of the source server, then import it to the **Policy Catalog** page on the target server.

Tasks

- Exporting a single policy
- Exporting all policies of a product
- Importing policies

Exporting a single policy

Use this task to export a policy to an XML file. Use this file to import the policy to another ePO server, or to keep as a backup of the policy.

Task

For option definitions, click **?** on the page displaying the options.

1 Go to **Systems | Policy Catalog**, then select the **Product** and **Category** from the drop-down lists. All created policies for that category appear in the details pane.
2 Locate the desired policy, then click **Export** next to the policy. The **Download File** page appears.
3 Right-click the link and select **Save Target As**.
4 Name the policy XML file and save it to a location. Ensure that this location is accessible to the target ePolicy Orchestrator server.

Exporting all policies of a product

Use this task to export all policies of a product to an XML file. Use this file to import the policy to another ePO server, or to keep as a backup of the policies.

Task

For option definitions, click **?** on the page displaying the options.

1 Go to **Systems | Policy Catalog**, then select the **Product** and **Category** . All created policies for that category appear in the details pane.
2 Click **Export** next to **Product policies** at the top of the page. The **Download File** page appears.
3 Right-click the link and select **Save Target As**.
4 Name the policy XML file and save it to the desired location. Ensure that this location is accessible to the target ePolicy Orchestrator server.

Importing policies

Use this task to import a policy XML file. Regardless of whether you exported a single policy, or all named policies, the import procedure is the same.

Task

For option definitions, click **?** on the page displaying the options.

1. Go to **Systems | Policy Catalog**, then click **Import** next to **Product policies** at the top of the page.
2. Browse to and select the desired policy XML file, then click **OK**.

The imported policies are added to the Policy Catalog.

Assigning a policy to a group of the System Tree

Use this task to assign a policy to a specific group of the System Tree. You can assign policies before or after a product is deployed.

Task

For option definitions, click **?** on the page displaying the options.

1. Go to **Systems | System Tree | Policies**, then select the desired **Product**. Each assigned policy per category appears in the details pane.
2. Locate the desired policy category, then click **Edit Assignment**. The **Policy Assignment** page appears.
3. If the policy is inherited, select **Break inheritance and assign the policy and settings below** next to **Inherited from**.
4. Select the desired policy from the **Assigned policy** drop-down list.

   NOTE: From this location, you can also edit the selected policy's settings, or create a new policy.

5. Choose whether to lock policy inheritance. Locking policy inheritance prevents any systems that inherit this policy from having another one assigned in its place.
6. Click **Save**.

Assigning a policy to a managed system

Use this task to assign a policy to a specific managed system. You can assign policies before or after a product is deployed.

Task

For option definitions, click **?** on the page displaying the options.

1. Go to **Systems | System Tree | Systems**, then select the desired group under **System Tree**. All the systems within this group (but not its subgroups) appear in the details pane.
2. Select the desired system, then click **Modify Policies on a Single System**. The **Policy Assignment** page for that system appears.
3. Select the desired **Product**. That product's policy categories are listed with the system's assigned policy.

4 Locate the desired policy category, then click **Edit Assignment**.

5 If the policy is inherited, select **Break inheritance and assign the policy and settings below** next to **Inherited from**.

6 Select the desired policy from the **Assigned policy** drop-down list.

NOTE: From this location, you can also edit the selected policy's settings, or create a new policy.

7 Choose whether to lock policy inheritance.

8 Click **Save**.

Assigning a policy to multiple managed systems within a group

Use this task to assign a policy to multiple managed systems within a group. You can assign policies before or after a product is deployed.

Task

For option definitions, click **?** on the page displaying the options.

1 Go to **Systems | System Tree | Systems**, then select the desired group in the System Tree. All the systems within this group (but not its subgroups) appear in the details pane.

2 Select the desired systems, then click **Assign Policy**. The **Assign Policies** page appears.

3 Select the **Product, Category,** and **Policy** from the drop-down lists, then click **Save**.

Enforcing policies for a product on a group

Use this task to enable or disable policy enforcement for a product on a System Tree group. Policy enforcement is enabled by default, and is inherited in the System Tree.

Task

For option definitions, click **?** on the page displaying the options.

1 Go to **Systems | System Tree | Policies**, then select the desired group in the System Tree.

2 Select the desired **Product**, then click the blue text next to **Enforcement Status**. The **Enforcement** page appears.

3 If you want to change the enforcement status you must first select **Break inheritance and assign the policy and settings below**.

4 Next to **Enforcement status**, select **Enforcing** or **Not enforcing** accordingly.

5 Choose whether to lock policy inheritance. This prevents systems that inherit this policy from having a different policy assigned in its place.

6 Click **Save**.

Enforcing policies for a product on a system

Use this task to enable or disable policy enforcement for a product on a system. Policy enforcement is enabled by default, and is inherited in the System Tree.

Task

For option definitions, click **?** on the page displaying the options.

1. Go to **Systems | System Tree | Systems**, then select the group under **System Tree** to which the system belongs. The list of systems belonging to this group appears in the details pane.
2. Select the desired system, then click **Modify Policies on a Single System**. The **Policy Assignment** page appears.
3. Select the desired **Product**, then click the blue text next to **Enforcement status**. The **Enforcement** page appears.
4. If you want to change the enforcement status you must first select **Break inheritance and assign the policy and settings below**.
5. Next to **Enforcement status**, select **Enforcing** or **Not enforcing** accordingly.
6. Click **Save**.

Copying and pasting assignments

Use these tasks to copy and paste policy assignments from one group or system to another. This is an easy way to share multiple assignments between groups and systems from different portions of the System Tree.

Tasks

- Copying policy assignments from a group
- Copying policy assignments from a system
- Pasting policy assignments to a group
- Pasting policy assignments to a specific system

Copying policy assignments from a group

Use this task to copy policy assignments from a group in the System Tree.

Task

For option definitions, click **?** on the page displaying the options.

1. Go to **Systems | System Tree | Policies**, then select the desired group under **System Tree**.
2. In the details pane, click **Copy Assignments**.
3. Select the products or features for which you want to copy policy assignments, then click **OK**.

Copying policy assignments from a system

Use this task to copy policy assignments from a specific system.

Task

For option definitions, click **?** on the page displaying the options.

1. Go to **Systems | System Tree | Systems**, then select the desired group under **System Tree**. The systems belonging to the selected group appear in the details pane.

2 Select the desired system, then click **Modify Policies on a Single System**.

3 Click **Copy Assignments**, then select the desired products or features for which you want to copy policy assignments, then click **OK**.

Pasting policy assignments to a group

Use this task to paste policy assignments to a group. You must have already copied policy assignments from a group or system.

Task

For option definitions, click **?** on the page displaying the options.

1 Go to **Systems | System Tree | Policies**, then select the desired group in the System Tree.

2 In the details pane, click **Paste Assignments**. If the group already has policies assigned for some categories, the **Override Policy Assignments** page appears.

3 Select the policy categories you want to replace with the copied policies, then click **OK**.

Pasting policy assignments to a specific system

Use this task to paste policy assignments to a specific system. You must have already copied policy assignments from a group or system.

Task

For option definitions, click **?** on the page displaying the options.

1 Go to **Systems | System Tree | Systems**, then select the desired group of the System Tree. All of the systems belonging to the selected group appear in the details pane.

2 Select the system where you want to paste policy assignments, then click **Modify Policies on a Single System**.

3 In the details pane, click **Paste Assignment**. If the system already has policies assigned for some categories, the **Override Policy Assignments** page appears.

NOTE: When pasting policy assignments, an extra policy appears in the list (Enforce Policies and Tasks), This policy controls the enforcement status of other policies.

4 Confirm the replacement of assignments.

Working with client tasks

Use these tasks to create and maintain client tasks.

Tasks

- Creating and scheduling client tasks
- Editing client tasks
- Deleting client tasks

Creating and scheduling client tasks

Use this task to create and schedule a client task. The process is similar for all client tasks.

Task

For option definitions, click **?** on the page displaying the options.

1. Go to **Systems | System Tree | Client Tasks**, select the desired group in the System Tree, then click **New Task**.
2. Type a name for the task you are creating, add any notes, then select the product and task type from the drop-down lists. For example, **Update**.
3. Select whether the schedule is enabled, then click **Next**. The **Configuration** page appears. This page of the wizard and its options depend on the task type selected.
4. Configure the settings, then click **Next**. The **Schedule** page appears.
5. Schedule the task as needed, then click **Next**.. The **Summary** page appears.
6. Review the task settings, then click **Save**.

The task is added to the list of client tasks for the selected group and any group that inherits the task.

Editing client tasks

Use this task to edit a client task's settings or schedule information for any exisitng task.

Task

For option definitions, click **?** on the page displaying the options.

1. Go to **Systems | System Tree | Client Tasks**, then select a desired group in the System Tree.
2. Click **Edit** next to the task. The **Client Task Builder** wizard appears.
3. Edit the task settings as needed, then click **Save**.

The managed systems receive these changes the next time the agents communicate with the server.

Deleting client tasks

Use this task to delete unneeded client tasks. You can delete any client task you have created, except for the deployment task.

Task

For option definitions, click **?** on the page displaying the options.

1. Go to **Systems | System Tree | Client Tasks**, then select the desired group in the System Tree.
2. Click **Delete** next to the desired client task.
3. Click **OK**.

Frequently asked questions

What is a policy?

A policy is a customized subset of product settings corresponding to a policy category. You can create, modify, or delete as many named policies as needed for each policy category.

What are the McAfee Default and My Default policies?

Upon installation, each policy category contains at least two policies. These are named McAfee Default and My Default. These are the only policies present for first-time installations. The configurations for both, initially, are the same.

The McAfee Default named policies cannot be edited, renamed, or deleted. The My Default policies can be edited, renamed, and deleted.

What happens to the child groups and systems of the group where I assigned a new policy?

All child groups and systems that are set to inherit the specific policy category, inherit the policy applied to a parent group.

How are the groups and systems where a policy is applied affected when the policy is modified in the Policy Catalog?

All groups and systems where a policy is applied receive any modification made to the policy at the next agent-server communication. The policy is then enforced at each policy enforcement interval.

I assigned a new policy, but it's not being enforced on the managed systems. Why?

New policy assignments are not enforced until the next agent-server communication.

I pasted policy assignments from one group or system (source) to another (target), but the policies assigned to the target location are not the same as the source location. Why not?

When you copy and paste policy assignments, only true assignments are pasted. If the source location was inheriting a policy that you selected to copy, then it is the inheritance characteristic that was pasted to the target, so the target then inherits the policy (for that particular policy category) from its parent, which may be a different policy than the one that was inherited onto the source.

Deploying Software and Updates

In addition to managing security products, ePolicy Orchestrator can deploy products to your network systems. Use ePolicy Orchestrator to deploy products and their updates.

If you plan to deploy security products and updates with a tool other than ePolicy Orchestrator, skip this section.

Are you deploying packages for the first time?

When deploying packages for the first time:

1. Understand product deployment and the types of packages that ePolicy Orchestrator can deploy.
2. Configure pull and replication tasks.
3. Configure deployment and update tasks.
4. Check in product and update packages to the master repository.

Contents

- Deployment packages for products and updates
- Product and update deployment
- Checking in packages manually
- Using the Product Deployment task to deploy products to managed systems
- Deploying update packages automatically with global updating
- Deploying update packages with pull and replication tasks
- Configuring agent policies to use a distributed repository
- Using local distributed repositories that are not managed
- Checking in engine, DAT and EXTRA.DAT update packages manually
- Updating managed systems regularly with a scheduled update task
- Confirming that clients are using the latest DAT files
- Evaluating new DATs and engines before distribution
- Manually moving DAT and engine packages between branches
- Deleting DAT or engine packages from the master repository

Deployment packages for products and updates

The ePolicy Orchestrator deployment infrastructure supports deploying products and components, as well as updating both.

Each McAfee product that ePolicy Orchestrator can deploy provides a product deployment package ZIP file. ePolicy Orchestrator can deploy these packages to any of your managed systems, once they are checked in to the master repository. The ZIP file contains the product installation files, which are compressed in a secure format.

ZIP files are used for both detection definition (DAT) and engine update packages.

You can configure product policy settings before or after deployment. McAfee recommends configuring policy settings before deploying the product to network systems. This saves time and ensures that your systems are protected as soon as possible.

These package types can be checked in to the master repository with pull tasks, or manually.

Supported package types

Package type	Description	Origination
Detection definition (DAT) files File type: ZIP	The regular, daily DAT files released by McAfee.	McAfeeFtp and McAfeeHttp update sites, and the McAfee website. Use a pull task to download DAT files directly into the master repository, or download and check them into the master repository manually.
Scanning engine File type: ZIP	The updated scanning engine for McAfee anti-virus products, such as VirusScan Enterprise. Engines are usually updated once or twice a year.	McAfeeFtp and McAfeeHttp update sites, and the McAfee website. Use a pull task to download engine files directly into the master repository, or download and check them into the master repository manually.
SuperDAT (SDAT.EXE) files File type: SDAT.EXE	The SuperDAT files contain both DAT and engine files in one update package. If bandwidth is a concern, McAfee recommends updating DAT and engine files separately.	McAfee website. Download and check SuperDAT files into the master repository manually.
Supplemental detection definition (EXTRA.DAT) files File type: EXTRA.DAT	The EXTRA.DAT files address one or a few specific threats that have appeared since the last DAT file was posted. If the threat has a high severity, distribute the EXTRA.DAT immediately, rather than wait until that signature is added to the next DAT file. EXTRA.DAT files are from the McAfee website. You can distribute them through ePolicy Orchestrator. Pull tasks do not retrieve EXTRA.DAT files.	McAfee website. Download and check supplemental virus definition files in to the master repository manually.
Product deployment packages File type: ZIP	A product deployment package contains the installation software of a McAfee product.	Product CD or downloaded product ZIP file. Check product deployment packages in to the master repository manually. For specific locations, see the documentation for that product. Only the agent and System Compliance Profiler deployment packages are checked in to the master repository as part of the ePO server installation.
Agent installation package File type: ZIP	An agent installation package contains the installation software for the agent.	Master repository — checked in at installation. For future versions of the agent, you must check agent installation packages in to the master repository manually.
Agent language packages File type: ZIP	An agent language package contains files necessary to display agent information in a local language.	Master repository — checked in at installation. For future versions of the agent, you must check agent language

Package type	Description	Origination
		packages into the master repository manually.

Package signing and security

All packages created and distributed by McAfee are signed with a key pair using the DSA (Digital Signature Algorithm) signature verification system, and are encrypted using 168-bit 3DES encryption. A key is used to encrypt or decrypt sensitive data.

You are notified when you check in packages that are not signed by McAfee. If you are confident of the content and validity of the package, continue with the checkin. These packages are secured in the same manner described above, but are signed by ePolicy Orchestrator when they are checked in.

Digital signatures guarantee that packages originated from McAfee or were checked in by you, and that they have not been tampered with or corrupted. The agent only trusts package files signed by ePolicy Orchestrator or McAfee. This protects your network from receiving packages from unsigned or untrusted sources.

Legacy product support (NetShield for Netware)

Older products use a flat directory structure to install product updates. Currently, this is limited to NetShield for NetWare.

If the update location you specify in the task settings is a distributed repository managed by ePolicy Orchestrator, you must enable NetShield for Netware support when you check the corresponding package in to the master repository. Doing so copies the packages into both directory structures, enabling you to support legacy products.

Package ordering and dependencies

If one product update is dependent on another, you must check their packages in to the master repository in the required order. For example, if Patch 2 requires Patch 1, you must check in Patch 1 before Patch 2. Packages cannot be reordered once they are checked in. You must remove them and check them in again, in the proper order. If you check in a package that supersedes an existing package, the existing package is removed automatically.

Product and update deployment

The ePO repository infrastructure allows you to deploy product and update packages to your managed systems from a central location. Although the same repositories are used, there are differences.

Comparison of product deployment and update packages

Product deployment packages	Update packages
Must be manually checked in to the master repository.	DAT and engine update packages can be copied from the source site automatically with a pull task. All other update packages must be checked int o the master repository manually.
Can be replicated to the distributed repositories and installed on managed systems with global updating.	Can be replicated to the distributed repositories and installed on managed systems automatically with global updating.

Product deployment packages	Update packages
If not implementing global updating for product deployment, a deployment task must be configured and scheduled for managed systems to retrieve the package.	If not implementing global updating for product updating, an update client task must be configured and scheduled for managed systems to retrieve the package.

Product deployment and updating process

Follow this high-level process for distributing DAT and engine update packages follows:

1. Check the update package in to the master repository with a pull task or manually.
2. If using global updating, nothing else is necessary, provided global updating has been configured and enabled.

   If not using global updating, use a replication task to copy the contents of the master repository to the distributed repositories.
3. If not using global updating, create and schedule an update or deployment task for agents to retrieve and install the update on managed systems.

Deployment tasks

Once you have checked in the product deployment package, use the Product Deployment client task to install the product on managed systems. The task installs any product that is deployable through ePolicy Orchestrator and has been checked in to the master repository.

Best practices

You can run the product deployment task for any group or individual system. When deciding how to stage your product deployment, McAfee recommends considering the size of the package and the available bandwidth between the master or distributed repositories and the managed systems. In addition to potentially overwhelming the ePO server or your network, deploying products to many systems can make troubleshooting problems more complicated.

Consider a phased rollout to install products to groups of systems at a time. If your network links are fast, try deploying to several hundred clients at a time. If you have slower or less reliable network connections, try smaller groups. As you deploy to each group, monitor the deployment, run reports to confirm successful installations, and troubleshoot any problems with individual systems.

If you are deploying McAfee products or components that are installed on a subset of your managed systems:

1. Use a tag to identify these systems.
2. Move the tagged systems to a group.
3. Configure a Product Deployment client task for the group.

Update tasks

Once an update package has been checked into the master repository and replicated to the distributed repositories, the agents on the managed systems still need to know when to go to the distributed repositories for updates. This is unnecessary if you are using global updating.

You can create and configure update client tasks to control when and how managed systems receive update packages. If you are not using global updating, creating these tasks are the only way you can control client updating with ePolicy Orchestrator.

If you are using global updating, this task is unnecessary, although you can create a daily task for redundancy.

Considerations when creating update client tasks

Consider the following when scheduling client update tasks:

- Create an Update client task to update DAT and engine files daily at the highest level of the System Tree that is inherited by all systems. If your organization is large, you can use randomization intervals to mitigate the bandwidth impact. Also, for large networks with offices in different time zones, run the task at the local system time on the managed system, rather than at the same time for all systems, to help balance network load.
- Schedule the task at least an hour after the scheduled replication task, if you are using scheduled replication tasks.
- Run update tasks for DAT and engine files at least once a day. Managed systems might be logged off from the network and miss the scheduled task; running the task frequently ensures these systems receive the update.
- Maximize bandwidth efficiency and create several scheduled client update tasks that update separate components and run at different times. For example, you can create one task to update only DAT files, then create another to update both DAT and engine files weekly or monthly — engine packages are released less frequently.
- Create and schedule additional tasks to update products that do not use the agent for Windows.
- Create a task to update your main workstation applications, such as VirusScan Enterprise, to ensure they all receive the update files. Schedule it to run daily or several times a day.

Global updating

McAfee recommends using global updating with your updating strategy. Global updating automates replication to your distributed repositories and updating managed systems. Replication and update tasks are not required. Checking contents in to your master repository initiates a global update. The entire process should complete within an hour in most environments.

Additionally, you can specify which packages and updates initiate a global update. However, when you only specify that certain content initiates a global update, ensure that you create a replication task to distribute content that was not selected to initiate a global update.

NOTE: When using global updating, McAfee recommends scheduling a regular pull task (to update the master repository) at a time when network traffic is minimal. Although global updating is much faster than other methods, it increases network traffic during the update.

Global updating process

Global updating updates most environments within an hour using this process:

1. Contents are checked in to the master repository.
2. Contents of the master repository are replicated automatically to the distributed repositories.
3. A SuperAgent wake-up call is broadcast to all SuperAgents, which then send the wake-up call to all agents within each SuperAgent's broadcast segment. The call contains information about the updated packages and the repositories containing them. If a package the managed systems require is in the wake-up call, the agents go to a distributed repository to get the package.
4. All agents go to their distributed repositories for new updates.

Requirements

These requirements must be met to implement global updating:

- A SuperAgent must use the same agent-server secure communication key as the agents that receive its wake-up call.
- A SuperAgent is installed on each broadcast segment. Managed systems cannot receive a SuperAgent wake-up call if there is no SuperAgent on the same broadcast segment. Global updating utilizes the SuperAgent wake-up call to alert agents that new updates are available.
- Distributed repositories are set up and configured throughout your environment. McAfee recommends SuperAgent repositories, but they are not required — global updating functions with all types of distributed repositories.
- If using SuperAgent repositories, managed systems must be able to "see" the repository from which it updates. Although, a SuperAgent is required on each broadcast segment for systems to receive the wake-up call, SuperAgent repositories are not required on each broadcast segment, but the managed systems must "see" the SuperAgent repository from which to update.

Pull tasks

Use pull tasks to update your master repository with DAT and engine update packages from the source site. DAT and engine files must be updated often. McAfee releases new DAT files daily and engine files less frequently. Deploy these packages to managed systems as soon as possible to protect them against the latest threats.

With this release, you can specify which packages are copied from the source site to the master repository.

NOTE: EXTRA.DAT files must be checked in to the master repository manually. They are available from the McAfee website.

A scheduled Repository Pull server task runs automatically and regularly at times and days you specify. For example, you can schedule a weekly Repository Pull task at 5:00 a.m. every Thursday.

You can also use the Pull Now task to check updates in to the master repository immediately. For example, when McAfee alerts you to a fast-spreading virus and releases a new DAT file to protect against it.

If a pull task fails you must check the packages in to the master repository manually.

Once you have updated your master repository, you can distribute these updates to your systems automatically with global updating or with replication tasks.

Considerations when scheduling a pull task

Consider these when scheduling pull tasks:

- Bandwidth and network usage. If you are using global updating, as recommended, schedule a pull task to run when bandwidth usage by other resources is low. With global updating, the update files are distributed automatically after the pull task finishes.
- Frequency of the task. DAT files are released daily, but you may not want to use your resources daily for updating.
- Replication and update tasks. Schedule replication tasks and client update tasks to ensure the update files are distributed throughout your environment.

Replication tasks

Use replication tasks to copy the contents of the master repository to distributed repositories. Unless you have replicated master repository contents to all your distributed repositories, some systems do not receive them. Ensure all your distributed repositories are up-to-date.

NOTE: If you are using global updating for all of your updates, replication tasks may not be necessary for your environment, although they are recommended for redundancy. However, if you are not using global updating for any of your updates, you must schedule a Repository Replication server task or run a Replicate Now task.

Scheduling regular Repository Replication server tasks is the best way to ensure that your distributed repositories are up-to-date. Scheduling daily replication tasks ensures that managed systems stay up-to-date. Using Repository Replication tasks automates replication to your distributed repositories.

Occasionally, you may check in files to your master repository that you want to replicate to distributed repositories immediately, rather than wait for the next scheduled replication. Run a Replicate Now task to update your distributed repositories manually.

Full vs. incremental replication

When creating a replication task, select **Incremental replication** or **Full replication**. Incremental replication uses less bandwidth and copies only the new updates in the master repository that are not yet in the distributed repository. Full replication copies the entire contents of the master repository.

TIP: McAfee recommends scheduling a daily incremental replication task. Schedule a weekly full replication task if it is possible for files to be deleted from the distributed repository outside of ePolicy Orchestrator's own replication functionality.

Repository selection

New distributed repositories are added to the repository list file containing all available distributed repositories. The agent of a managed system updates this file each time it communicates with the ePO server. The agent performs repository selection each time the agent (**McAfee Framework Service**) service starts and when the repository list changes.

Selective replication provides more control over the updating of individual repositories. When scheduling replication tasks, you can choose:

- Specific distributed repositories to which the task applies. Replicating to different distributed repositories at different times lessens the impact on bandwidth resources. These repositories can be specified when you create or edit the replication task.
- Specific files and signatures that are replicated to the distributed repositories. Selecting only those types of files that are necessary to each system that checks into the distributed repository lessens the impact on bandwidth resources. When you define or edit your distributed repositories, you can choose which packages you want to replicate to the distributed repository.

NOTE: This functionality is intended for updating products that are installed only on several systems in your environment, like GroupShield and WebShield. The functionality allows you to distribute these updates only to the distributed repositories these systems use.

How agents select repositories

By default, agents can attempt to update from any repository in the repository list file. The agent can use a network ICMP ping or subnet address compare algorithm to find the distributed repository with the quickest response time. Usually, this is the distributed repository closest to the system on the network.

You can also tightly control which distributed repositories agents use for updating by enabling or disabling distributed repositories in the agent policy settings. McAfee does not recommend disabling repositories in the policy settings. Allowing agents to update from any distributed repository ensures they receive the updates.

Server Task Log

The server task log prvides information about your pull and replication tasks, in addition to all server tasks. This provides the status of the task and any errors that may have occurred.

Replication task information in the server task log

The following information is available for replication tasks on the **Reporting | Server Task Log** tab:

- Start date and task duration.
- Status of task at each site (when expanded).
- Any errors or warnings, their codes, and the site to which they apply.

Pull task information in the server task log

The following information is available for pull tasks on the **Reporting | Server Task Log** tab:

- Start date and task duration.
- Any errors or warnings and their codes.
- Status of each package that is checked into the master repository.
- Information regarding any new packages that are being checked into the master repository.

Checking in packages manually

Use this task to manually check in the deployment packages to the master repository so that ePolicy Orchestrator can deploy them.

Before you begin

You must have the appropriate permissions to perform this task.

NOTE: You cannot check in packages while pull or replication tasks are running.

Task

For option definitions, click **?** on the page displaying the options.

1 Go to **Software | Master Repository**, then click **Check In Package**. The **Check In Package** wizard appears.

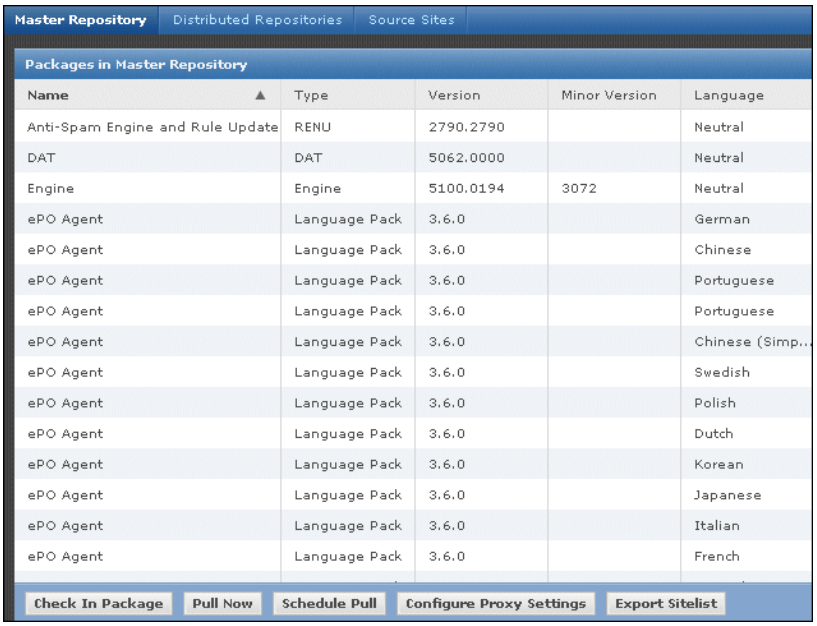

Figure 24: Master Repository tab

2 Select the package type, then browse to and select the desired package file.

3 Click **Next**. The **Package Options** page appears.

4 Next to **Check in package to this branch**, select the desired branch.

If there are requirements in your environment to test new packages before deploying them throughout the production environment, McAfee recommends using the Evaluation branch whenever checking in packages. Once you finish testing the packages, you can move them to the Current branch on the **Software | Master Repository** tab.

5 Next to **Options**, select whether to:

- **Support Netshield for NetWare** — Select this option if you are checking in a package for NetShield for Netware.
- **Move the existing package to the Previous branch** — Moves the existing package of the same type (but different version) to the Previous branch when the new package is checked in.

6 Click **Save** to begin checking in the package. Wait while the package checks in.

The new package appears in the **Packages in Master Repository** list on the **Master Repository** tab.

Using the Product Deployment task to deploy products to managed systems

Use these tasks to deploy products to managed systems with the Product Deployment client task. ePolicy Orchestrator 4.0.2 allows you to create this task for a single system, or for groups of the System Tree.

Tasks

- Configuring the Deployment task for groups of managed systems
- Configuring the Deployment task to install products on a managed system

Configuring the Deployment task for groups of managed systems

Use this task to configure the Product Deployment task to deploy products to groups of managed systems in the System Tree.

Task

For option definitions, click **?** on the page displaying the options.

1. Go to **Systems | System Tree | Client Tasks**, then select a group in the System Tree.
2. Click **New Task**, then name the task and select **Product Deployment (McAfee Agent)** from the **Task type** drop-down list.
3. Add any descriptive information to the **Notes** field.

   The information you add here is only visible when you open the task at this group or a child group that inherits the task from this group.
4. Click **Next**. The **Configuration** page appears.
5. Select the desired platforms to which you are deploying the packages.
6. Next to **Products to deploy**, select the desired product from the first drop-down list.

   The products listed are those for which you have already checked in a package to the master repository. If you do not see the product you want to deploy listed here, you must first check in that product's package.
7. Set the **Action** to **Install**, then select the language version of the package.
8. To specify command-line installation options, type the desired command-line options in the **Command line** text field. See the product documentation for information on command-line options of the product you are installing.
9. Click **Next**. The **Schedule** page appears.
10. Schedule the task as needed, then click **Next**. The **Summary** page appears.
11. Review and verify the details of the Product Deployment task, then click **Save**.

Configuring the Deployment task to install products on a managed system

Use this task to deploy products to a single system using the Product Deployment task.

Create a Product Deployment client task for a single system when that system requires:

- A product installed which other systems within the same group do not require.
- A different schedule than other systems in the group. For example, if a system is located in a different time zone than its peers.

Task

For option definitions, click **?** on the page displaying the options.

1 Go to **Systems | System Tree | Systems**, then select the group in the System Tree which contains the desired system.
2 Select the checkbox next to the desired system.
3 Click **Modify Tasks on a Single System**. The list of tasks assigned to this system appears.

   NOTE: You may need to click **More Actions** to access **Modify Tasks on a Single System**.

4 Click **New Task** . The **Description** page of the **Client Task Builder** appears.
5 Select **Product Deployment (McAfee Agent)** from the **Type** drop-down list.
6 Add any descriptive information to the **Notes** field.

   The information you add here is only visible when you open the task at the system for which you are configuring the task.

7 Next to **Inheritance**, select whether this system should inherit the task's schedule and settings from the parent group of the System Tree.
8 Select **McAfee Agent** from the **Product** drop-down list, then select **Product Deployment** from the **Type** drop-down list.
9 Click **Next**. The **Configuration** page appears.
10 Select the desired platforms to which you are deploying the packages.
11 Next to **Products** to deploy, select the desired product from the first drop-down list.

   The products listed are those for which you have already checked in a package file to the master repository. If you do not see the product you want to deploy listed here, you must first check in that product's package file.

12 Set the **Action** to **Install**, then select the language version of the package.
13 To specify command-line install options, type the desired command-line options in the **Command line** text field. See the product documentation for information on command-line options of the product you are installing.
14 Click **Next**. The **Schedule** page appears.
15 Schedule the task as needed, then click **Next**. The **Summary** page appears.
16 Review and verify the details of the Product Deployment task, then click **Save**.

Deploying update packages automatically with global updating

Use this task to enable global updating on the server. Global updating automatically deploys user-specified update packages to managed systems.

Before you begin

- Repositories must be created and available to all agents that receive the SuperAgent wake-up call.
- There must be a SuperAgent in each broadcast segment that contains agents you want to receive the SuperAgent wake-up call.
- Only global administrators can perform this task.

Task

For option definitions, click **?** on the page displaying the options.

1 Go to **Configuration | Server Settings**, select **Global Updating**, then click **Edit** at the bottom of the page.

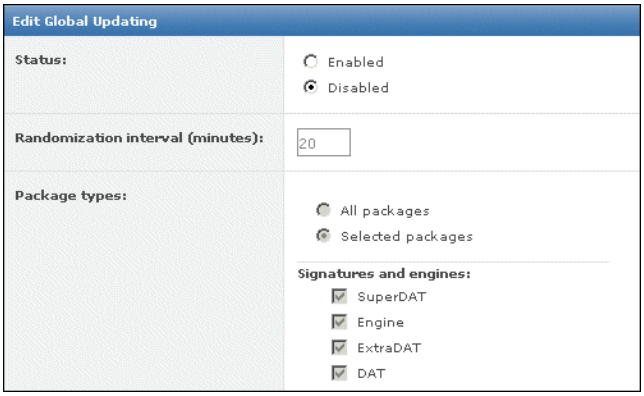

Figure 25: Edit Global Updating page

2 On the **Edit Global Updating** page, select **Enabled** next to **Status**.

3 Edit the **Randomization interval**, if desired. The default is **20 minutes**.

Each client update occurs at a randomly selected time within the randomization interval, which helps distribute network load. For example, if you update 1000 clients using the default randomization interval of 20 minutes, roughly 50 clients update each minute during the interval, lowering the load on your network and on your server. Without the randomization, all 1000 clients would try to update simultaneously.

4 Next to **Packages types**, select which packages initiate an update.

Global updating initiates an update only if new packages for the components specified here are checked in to the master repository or moved to another branch. Select these components carefully.

5 When finished, click **Save**.

Once enabled, global updating initiates an update the next time you check in any of the selected packages or move them from to another branch.

NOTE: Be sure to run a Pull Now task and schedule a recurring Repository Pull server task, when you are ready for the automatic updating to begin.

Deploying update packages with pull and replication tasks

Use these tasks to implement a task-based updating strategy once you have created your repository infrastructure. You must rely on these tasks if you are not using global updating in your environment.

Before you begin

Make sure repositories are created and in locations available to managed systems.

Tasks

- Using pull tasks to update the master repository
- Replicating packages from the master repository to distributed repositories

Using pull tasks to update the master repository

Use either of these tasks to update the contents of the master repository from the McAfee update site or a user-configured source site.

You can schedule pull tasks or run them immediately.

Before you begin

Ensure proxy settings are configured so that the master repository can access the source site.

Tasks

- Running a pull task on a schedule
- Running a Pull Now task

Running a pull task on a schedule

Use this task to schedule a recurring pull task that updates the master repository from the source site. Pull tasks now provide the ability to select which packages are copied from the source site.

Before you begin

You must have the appropriate permissions to perform this task.

Task

For option definitions, click **?** on the page displaying the options.

1. Go to **Software | Master Repository**, then click **Schedule Pull** at the bottom of the page. The **Description** page of the **Server Task Builder** wizard appears.
2. Name and describe the task.
3. Choose whether to enable or disable the task, then click **Next**. The **Actions** page appears.

   Disabled tasks can be run manually, but do not run at scheduled times.
4. Select **Repository Pull** from the drop-down list.

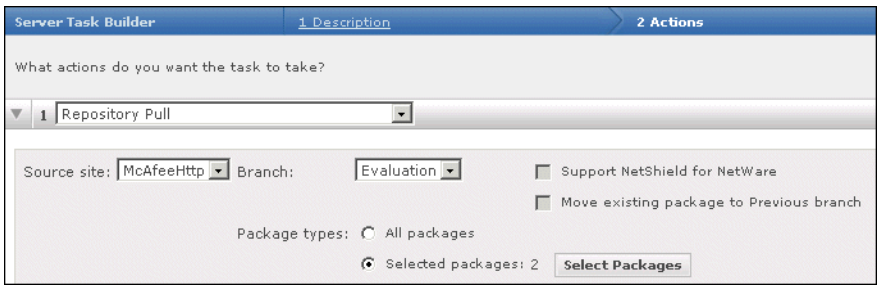

Figure 26: Repository Pull server task action

5. Select the source site from which to pull contents into the master repository.
6. Select the branch to receive the packages.

Select **Evaluation** to test the packages in a lab environment first.

Select **Current** to use the packages without testing them first.

7 Select whether to pull:

- **All packages**
- **Selected packages** — If you select this option, you must click **Select Packages** and choose the packages to pull from the source site when this task runs.

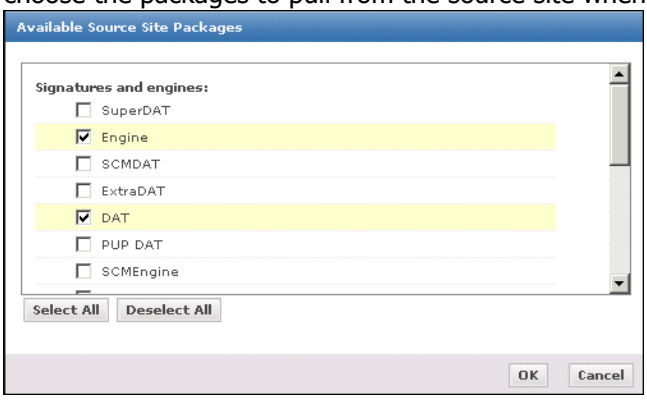

Figure 27: Available Source Site Packages dialog box

8 Select whether to:

- **Support NetShield for Netware**
- **Move existing packages of the same type to Previous branch**

9 Click **Next**. The **Schedule** page of the wizard appears.

10 Schedule the task as needed, then click **Next**. The **Summary** page appears.

NOTE: The **Schedule** page provides more flexibility than the scheduling functionality of previous versions. In addition to more granular scheduling in all of the schedule types, you can use cron syntax by selecting the **Advanced** schedule type.

11 Review the summary information, then click **Save**.

The scheduled Repository Pull task is added to the task list on the **Server Tasks** page.

Running a Pull Now task

Use this task to initiate a pull task that updates the master repository from the source site immediately. With this release, you can select which packages in the source site are copied to the master repository.

Before you begin

- You must have the appropriate software permissions to perform this task.
- Proxy settings must be configured to allow the master repository to access the source site.

Task

For option definitions, click **?** on the page displaying the options.

1 Go to **Software | Master Repository**, then click **Pull Now** at the bottom of the page. The Pull Now wizard appears.

2 Select the source site from the list of available repositories.

3 Select the repository branch that receives the packages.

   Select **Evaluation**, to test the packages in a lab environment first.

   Select **Current** to use the packages without first testing them.

4 Select **Support NetShield for NetWare** if you have NetShield for NetWare in your environment.

5 Select **Move existing packages of the same type to the Previous branch** to move the current package versions saved in the Current branch to the Previous branch.

6 Click **Next**. The **Package Selection** page appears.

7 Select which packages to copy from the source site, then click **Next**. The **Summary** page appears.

8 Verify the task details, then click **OK** to begin the pull task. The **Server Task Log** page appears, where you can monitor the status of the task until it finishes.

Replicating packages from the master repository to distributed repositories

Use either of these tasks to replicate contents of the master repository to distributed repositories. You can schedule a Repository Replication server task that occurs regularly, or run a Replicate Now task for immediate replication.

Tasks

- Running a Repository Replication server task on a schedule
- Running a Replicate Now task

Running a Repository Replication server task on a schedule

Use this task to create a scheduled Repository Replication server task.

Before you begin

- You must have appropriate permissions to perform this task.
- Your distributed repositories must be set up and added to ePolicy Orchestrator.

Task

For option definitions, click **?** on the page displaying the options.

1 Go to **Software | Distributed Repositories**, then click **Schedule Replication**. The **Description** page of the **Server Task Builder** wizard appears.

2 Name and describe the task.

3 Choose whether to enable or disable the task, then click **Next**. The **Actions** page appears.

   Disabled tasks can be run manually, but do not run at scheduled times.

4 Select **Repository Replication** from the drop-down list.

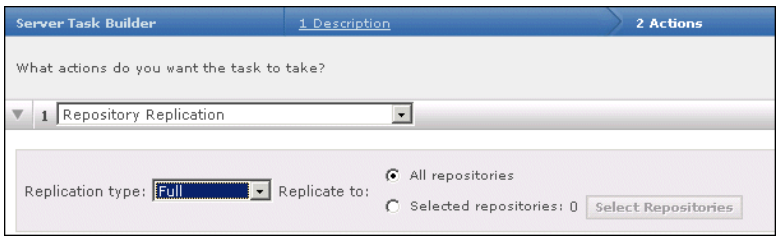

Figure 28: Repository Replication server task action

5 Select **Incremental** or **Full** from the **Replication type** drop-down list.

Incremental replicates only the differences between the master and distributed repositories.

Full replicates all contents of the master repository to the distributed repositories.

6 Select **All repositories** or **Selected repositories** next to **Replicate to**.

NOTE: If you select **Selected repositories**, you must click **Select Repositories** to choose which distributed repositories receive packages when this task is initiated.

7 Click **Next**. The **Schedule** page of the wizard appears.

8 Schedule the task as desired, then click **Next**. The **Summary** page appears.

NOTE: The **Schedule** page provides more flexibility than the scheduling functionality of previous versions. In addition to more granular scheduling in all of the schedule types, you can use cron syntax by selecting the **Advanced** schedule type.

9 Review the summary information, then click **Save**.

The scheduled Repository Pull task is added to the task list on the **Server Tasks** page.

Running a Replicate Now task

Use this task to replicate contents from the master repository to distributed repositories immediately.

Before you begin

- You must have appropriate permissions to perform this task.
- Any distributed repositories participating in the replication must be set up and added to ePolicy Orchestrator.

Task

For option definitions, click **?** on the page displaying the options.

1 Go to **Software | Distributed Repositories**, then click **Replicate Now**. The **Repositories** page of the **Replicate Now** wizard appears.

2 Select which distributed repositories participate in the replication, then click **Next**.

If you are not sure which distributed repositories need to be updated, replicate to them all.

3 Select **Incremental replication** or **Full replication**, then click **Next**.

NOTE: If this is the first time you are replicating to a distributed repository, it is a full replication even if you select incremental replication.

4 Click **Start Replication** to begin the task. The **Server Task Log** page appears, displaying the status of the task until it completes. Replication time depends on the changes to the master repository and the number of distributed repositories to which you are replicating.

After the task is complete, you can initiate an immediate client update task so managed systems in other locations can get updates from the distributed repositories.

Configuring agent policies to use a distributed repository

Use this task to customize how agents select distributed repositories.

Task

For option definitions, click **?** on the page displaying the options.

1 On the **Repositories** tab in the **McAfee Agent | General** policy pages, select **Use this repository list**.

2 Under **Repository selection**, specify the method to sort repositories:

- **Ping time** — Sends an ICMP ping to the closest five repositories (based on subnet value) and sorts them by response time.
- **Subnet value** — Compares the IP addresses of client systems and all repositories and sorts repositories based on how closely the bits match. The more closely the IP addresses resemble each other, the higher in the list the repository is placed.
- **User order in repository list** — Selects repositories based on their order in the list.

3 Disable repositories by deselecting the checkbox next to their name in the Repository list.

4 If you select **User defined list** in **Repository selection**, click **Move up** or **Move down** to specify the order in which you want client systems to select distributed repositories.

5 Click **Save** when finished.

Using local distributed repositories that are not managed

Use this task to copy and paste contents from the master repository into the unmanaged distributed repository. Once created, you must manually configure managed systems to go to the unmanaged repository for files.

Task

For option definitions, click **?** on the page displaying the options.

1 Copy all files and subdirectories in the master repository folder from the server. By default, this is in the following location on your server:

C:\Program Files\Mcafee\ePO\4.0.0\DB\Software

2 Paste the copied files and subfolders in your repository folder on the distributed repository system.

3 Configure an agent policy for managed systems to use the new unmanaged distributed repository:

   a Create a new agent policy or open an existing one for editing.

   CAUTION: Policy inheritance cannot be broken for tabs of a policy. Therefore, when you apply this policy to systems, ensure that only the desired systems receive and inherit the policy to use the unmanaged distributed repository.

   b Select the **Repositories** tab.

   c Click **Add** next to the **Repositories list**. The **Add Repository** page appears.

   d Type a name in the **Repository Name** text field. The name does not have to be the name of the system hosting the repository.

   e Under **Retrieve Files From**, select the type of repository.

   f Under **Configuration**, type the location you created using the appropriate syntax for the repository type.

   g Type a port number or keep the default port.

   h Configure authentication credentials as needed.

   i Click **OK** to add the new distributed repository to the list.

   j Select the new repository in the list.

   The type **Local** indicates it is not managed by ePolicy Orchestrator. When a non-managed repository is selected in the **Repository list**, the **Edit** and **Delete** buttons are enabled.

   k Click **Save**.

Any system to which this policy is applied receives the new policy at the next agent-server communication.

Checking in engine, DAT and EXTRA.DAT update packages manually

Use this task to manually check in the update packages to the master repository to deploy them using ePolicy Orchestrator. Some packages can only be checked in manually.

Before you begin

You must have appropriate permissions to perform this task.

NOTE: You cannot check in packages while pull or replication tasks are executing.

Task

For option definitions, click **?** on the page displaying the options.

1 Go to **Software | Master Repository**, then click **Check In Package**. The **Check In Package** wizard appears.

2 Select the package type, then browse to and select the desired package file.

3 Click **Next**. The **Package Options** page appears.

4 Next to **Branch**, select the desired branch.

   If your environment requires testing new packages before deploying them, McAfee recommends using the Evaluation branch. Once you finish testing the packages, you can move them to the Current branch on the **Software | Master Repository** tab.

5 Next to **Options**, select whether to:

   - **Support Netshield for NetWare** — Select this option if you are checking in a package for NetShield for NetWare.
   - **Move the existing package to the Previous branch** — Select this option if you want to move the existing package (of the same type that you are checking in) to the Previous branch.

6 Click **Save** to begin checking in the package. Wait while the package checks in.

The new package appears in the **Packages in Master Repository** list on the **Master Repository** page.

Updating managed systems regularly with a scheduled update task

Use this task to create and configure update tasks. If you are not using global updating., McAfee recommends using a daily Update client task to ensure systems are up-to-date with the latest DAT and engine files.

Task

For option definitions, click **?** on the page displaying the options.

1 Go to **Systems | System Tree | Client Tasks**, select the desired group in the System Tree to which you want the task to apply, then click **New Task**. The **Description** page of the **Client Task Builder** wizard appears.

2 Name and describe the task.

3 Select **Update (McAfee Agent)** from **Type** drop-down list, then click **Next**. The **Configuration** page appears.

4 Select whether to expose the **Update in Progress** dialog box to the end-users. If you select this option, you can also give the end-users the ability to postpone the update.

5 Click **Next**. The **Schedule** page appears.

6 Schedule the task as desired, then click **Next**. The **Summary** page appears.

7 Review the details of the task, then click **Save**.

The task is added to the list of client tasks for the groups and systems to which it is applied. Agents receive the new update task information the next time they communicate with the server. If the task is enabled, the update task runs at the next occurrence of the scheduled day and time. Each system updates from the appropriate repository, depending on how the policies for that client's agent are configured.

Confirming that clients are using the latest DAT files

Use this task to check the version of DAT files on managed systems.

Task

For option definitions, click **?** on the page displaying the options.

- Go to **Reporting | Queries**, select **VSE: DAT Deployment** in the **Queries** list, then click **Run Query**.

  NOTE: See the VirusScan Enterprise documentation for more information on this query.

Evaluating new DATs and engines before distribution

Use this task to test update packages using the Evaluation branch. You may want to test DAT and engine files on a few systems before deploying them to your entire organization.

ePolicy Orchestrator provides three repository branches for this purpose.

Task

For option definitions, click **?** on the page displaying the options.

1. Create a scheduled Repository Pull task that copies update packages in the Evaluation branch of your master repository. Schedule it to run after McAfee releases updated DAT files.
2. Create or select a group in the System Tree to serve as an evaluation group, and create a McAfee Agent policy for the systems to use only the Evaluation branch. (In the **Repository Branch Update Selection** section of the **Updates** tab.)

   The policies take affect the next time the agent calls into the server. The next time the agent updates, it retrieves them from the Evaluation branch.
3. Create a scheduled Update client task for the evaluation systems that updates DAT and engine files from the Evaluation branch of your repository. Schedule it to run one or two hours after your Repository Pull task is scheduled to begin.

   The evaluation update task created at the evaluation group level causes it to run only for that group.
4. Monitor the systems in your evaluation group until satisfied.
5. Move the packages from the Evaluation branch to the Current branch of your master repository using the **Change Branch** action on the **Software | Master Repository** tab. Adding them to the Current branch makes them available to your production environment. The next time any Update client tasks run that retrieves packages from the the Current branch, the new DAT and engine files are distributed to systems that use the task.

Manually moving DAT and engine packages between branches

Use this task to move packages manually between the Evaluation, Current, and Previous branches after they are checked in to the master repository.

Task

For option definitions, click **?** on the page displaying the options.

1. Go to **Software | Master Repository**. The **Packages in Master Repository** table appears.
2. In the row of the desired package, click **Change Branch**. The **Change Branch** page appears.
3. Select whether to move or copy the package to another branch.
4. Select which branch receives the package.

   NOTE: If you have NetShield for NetWare in your network, select **Support NetShield for NetWare**.

5. Click **OK**.

Deleting DAT or engine packages from the master repository

Use this task to delete packages from the master repository. As you check in new update packages regularly, they replace the older versions or move them to the Previous branch, if you are using the Previous branch. However, you may want to manually delete DAT or engine packages from the master repository.

Before you begin

You must have appropriate permissions to perform this task.

Task

For option definitions, click **?** on the page displaying the options.

1. Go to **Software | Master Repository**. The **Packages in Master Repository** table appears.
2. In the row of the desired package, click **Delete**. The **Delete Package** dialog box appears.
3. Click **OK**.

Sending Notifications

The ePolicy Orchestrator Notifications feature alerts you to events that occur on your managed systems or on the ePolicy Orchestrator server . You can configure notification rules in ePolicy Orchestrator to send email messages or SNMP traps, as well as run external commands when specific events are received and processed by the ePolicy Orchestrator server. The ability to specify the event categories that generate a notification message and the frequencies with which such messages are sent are highly configurable.

This feature is designed to notify specific individuals when the conditions of a rule are met. These include, but are not limited to:

- Detection of threats by your anti-virus software product. Although many anti-virus software products are supported, events from VirusScan Enterprise include the IP address of the source attacker so that you can isolate the system infecting the rest of your environment.
- Outbreak situations. For example, 1000 virus detected events are received within five minutes.
- High-level compliance of ePolicy Orchestrator server events. For example, a replication task was not completed.

You can also configure notification rules to execute commands and launch registered executables when the specified conditions are met.

Are you setting up Notifications for the first time?

When setting up Notifications for the first time:

1. Understand Notifications and how it works with the System Tree and your network.
2. Plan your implementation. Which users need to know about which events?
3. Define an SNMP server, registered executables, and external commands if you plan to implement Notifications features that use them.
4. Create notification rules.

Contents

- Notifications and how it works
- Planning
- Determining how events are forwarded
- Setting up ePO Notifications
- Creating and editing Notification rules
- Viewing the history of Notifications
- Product and component list
- Frequently asked questions

Notifications and how it works

Before you plan the implementation of Notifications, you should understand how this feature works with ePolicy Orchestrator and the System Tree.

NOTE: This feature does not follow the inheritance model of policy enforcement.

Events that occur on systems in your environment are delivered to the server, and the notification rules (associated with the group that contains the affected systems and each parent above it) are triggered by the events. If the conditions of any such rule are met, a notification message is sent, or an external command is run, per the rule's configurations.

This design allows you to configure independent rules at the different levels of the System Tree. These rules can have different:

- Thresholds for sending a notification message. For example, an administrator of a particular group wants to be notified if viruses are detected on 100 systems within 10 minutes on the group, but a global administrator does not want to be notified unless viruses are detected on 1000 systems within the entire environment in the same amount of time.
- Recipients for the notification message. For example, an administrator for a particular group wants to receive a notification message only if a specified number of virus detection events occur within the group. Or, a global administrator wants each group administrator to receive a notification message if a specified number of virus detection events occur within the entire System Tree.

Throttling and aggregation

You can configure when notification messages are sent by setting thresholds based on *aggregation* and *throttling*.

Aggregation

Use aggregation to determine the thresholds of events at which the rule sends a notification message. For example, configure the same rule to send a notification message when the server receives 100 virus detection events from different systems within an hour *and* whenever it has received 1000 virus detection events from any system.

Throttling

Once you have configured the rule to notify you of a possible outbreak, use throttling to ensure you do not receive too many notification messages. If you are administering a large network, then you may be receiving tens of thousands of events during an hour, creating thousands of notification messages based on such a rule. Notifications allows you to throttle the number of notification messages you receive based on a single rule. For example, you can specify in this same rule that you don't want to receive more than one notification message in an hour.

Notification rules and System Tree scenarios

To show how this feature functions with the System Tree, two scenarios are used.

For both scenarios, we can assume that each group of the System Tree has a similar rule configured. Each rule is configured to send a notification message when 100 virus detection events have been received from any product within 60 minutes. For reference purposes, each

rule is named **VirusDetected_<groupname>**, where <groupname> is the name of the group as it appears in the System Tree (for example, **VirusDetected_Subgroup2c**).

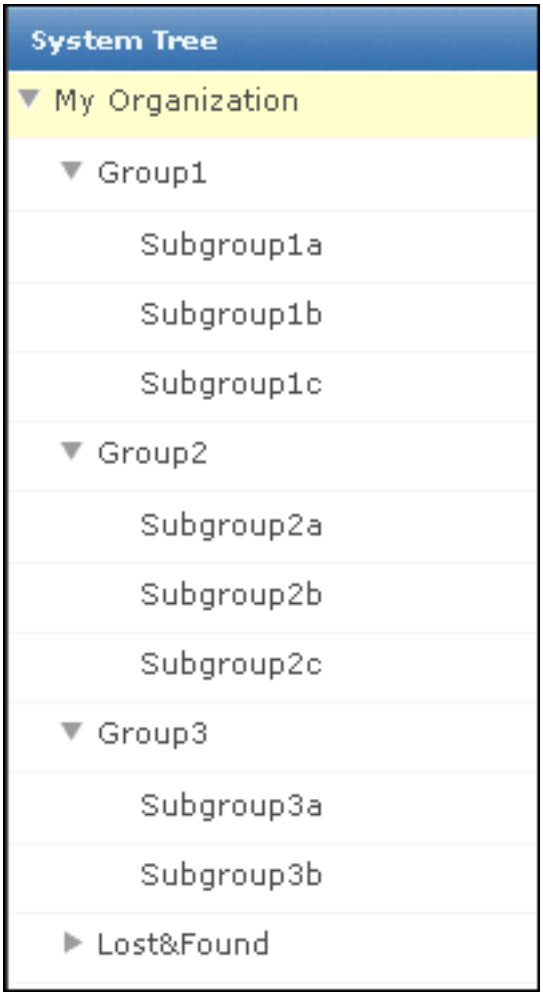

Figure 29: System Tree for Notification Scenarios

Scenario one

For this scenario, 100 virus detections are detected in **Subgoup2C** within 60 minutes in a single day.

Conditions of the rules **VirusDetected_Subgroup2C**, **VirusDetected_Group2**, and **VirusDetected_MyOrganization** are met, sending notification messages (or launching registered executables) per the rules' configurations.

Scenario two

For this scenario, 50 virus detections are detected in **Subgroup2C** and 50 virus infections are detected in **Subgroup3B** within 60 minutes in a single day.

Conditions of the **VirusDetected_MyOrganization** rule are met, sending notification messages (or launching registered executables) per the rules' configurations. This is the only rule that can be applied to all 100 events.

Default rules

ePolicy Orchestrator provides six default rules that you can enable for immediate use while you learn more about the feature.

NOTE: Once enabled, the default rules send notification messages to the email address you provided in the ePO installation wizard.

Before enabling any of the default rules:

- Specify the email server (at **Configuration | Server Settings**) from which the notification messages are sent.
- Ensure the recipient email address is the one you want to receive email messages. This address is configured on the **Notifications** page of the wizard.

Default notification rules

Rule Name	Associated Events	Configurations
Daily unknown product notification	Any events from any unknown products.	Sends a notification message at most, once a day.
Daily unknown category notification	Any event of an unknown category.	Sends a notification message at most, once a day.
Virus detected and not removed	**Virus Detected and Not Removed** events from any product.	Sends a notification message: • When the number of events exceeds 1000 within an hour. • At most, once every two hours. • With the source system IP address, actual threat names, and actual product information, if available. • When the number of affected systems is at least 500.
Virus detected heuristics and not removed	**Virus Detected (Heuristics) and Not Removed** events from any product.	Sends a notification message: • When the number of events exceeds 1000 within an hour. • At most, once every two hours. • With the source system IP address, actual threat names, and actual product information, if available. • When the number of affected systems is at least 500.
Repository update or replication failed	Repository update or replication failed	Sends a notification message when any events are received.
Non-compliant computer detected	**Non-Compliant Computer Detected** events.	Sends a notification message when any events are received from the Generate Compliance Event server task.

Planning

Before creating rules that send notifications, save time by planning:

- The types of events (product and server) that trigger notification messages in your environment.
- Who should receive which notification messages. For example, it may not be necessary to notify the administrator of group B about a failed replication in group A, but you may want all administrators to know that an infected file was discovered in group A.
- Which types and levels of thresholds you want to set for each rule. For example, you may not want to receive an email message every time an infected file is detected during an outbreak. Instead, you can choose to have such a message sent — at most — once every five minutes, regardless of how often that server is receiving the event.
- Which commands or registered executables you want to run when the conditions of a rule are met.

Determining how events are forwarded

Use these tasks to determine when events are forwarded and which events are forwarded immediately.

The server receives notifications from the agents. You must configure its policies to forward events either immediately to the server or only at agent-to-server communication intervals.

If you choose to send events immediately (as set by default), the agent forwards all events as soon as they are received. If you want all events sent to the server immediately so that they can be processed by Notifications when the events occur, configure the agent to send them immediately.

If you choose not to have all events sent immediately, the agent forwards only events immediately that are designated by the issuing product as high priority. Other events are sent only at the agent-server communication.

Tasks

- Determining which events are forwarded immediately
- Determining which events are forwarded

Determining which events are forwarded immediately

Use this task to determine whether events are forwarded immediately or only at the agent-to-server communication interval.

If the currently applied policy is not set for immediate uploading of events, either edit the currently applied policy or create a new McAfee Agent policy. This setting is configured on the **Events** tab.

Task

For option definitions click **?** on the page displaying the options.

1. Open the desired agent policy, then click **Events**.
2. Select **Enable priority event forwarding**.
3. Select the event severity. Events of the selected severity (and greater) are forwarded immediately to the server.
4. To regulate traffic, type an **Interval between uploads** (in minutes).

5 To regulate traffic size, type the **Maximum number of events per upload**.

6 Click **Save**.

Determining which events are forwarded

Use this task to determine which events are forwarded to the server.

Task

For option definitions click **?** on the page displaying the options.

1 Go to **Configuration | Server Settings**, select **Event Filtering**, then click **Edit** at the bottom of the page.

2 Select the desired events, then click **Save**.

These settings take effect once all of the agents have called in.

Setting up ePO Notifications

Use these tasks to configure the necessary resources to get the most out of Notifications.

Before using this feature, you must:

- Notifications permissions — Create or edit permission sets and ensure they are assigned to the appropriate ePO users.
- Email server — Configure the email (SMTP) server at **Configuration | Server Settings**.
- Email contacts list — Specify the list from which you select recipients of notification messages at **Configuration | Contacts**.
- SNMP servers — Specify a list of SNMP servers to use while creating rules. You can configure rules to send SNMP traps to SNMP servers when the conditions are met for a rule to initiate a notification message.
- External commands — Specify a list of external commands to run when the conditions of a rule are met.

Tasks

- Giving users appropriate permissions to Notifications
- Working with SNMP servers
- Working with registered executables and external commands

Giving users appropriate permissions to Notifications

Use this task to ensure all desired administrators have the appropriate permissions to Notifications.

Task

For option definitions click **?** on the page displaying the options.

1 Go to **Configuration | Permission Sets**.

2 Click **New Permission Set,** or select an existing one.

3 Next to **Notifications**, click **Edit**.

4 Select the desired Notifications permission:

- No permissions
- View notification rules and Notification Log

  NOTE: This permission also grants the ability to view SNMP servers, registered executables, and external commands.

- Create and edit notification rules; view Notification Log

  NOTE: This permission also grants the ability to view SNMP servers, registered servers, and external commands.

- Create and edit notification rules; view and purge Notification Log; create and edit SNMP servers and external commands

5 Click **Save**.

6 Repeat steps 2 through 4 until you have created and edited the necessary permission sets.

7 If you created a new permission set for this, go to **Configuration | Users**.

8 Select a user to whom you want to assign the new permission set, then click **Edit**.

9 Next to **Permission sets** select the checkbox next to the permission set with the desired Notifications permissions, then click **Save**.

10 Repeat steps 6 through 8 until all users are assigned the appropriate permissions.

Working with SNMP servers

Use these tasks to configure Notifications to use your SNMP server. You can configure Notifications to send SNMP (Simple Network Management Protocol) traps to your SNMP server, allowing you to receive SNMP traps at the same location where you can use your network management application to view detailed information about the systems in your environment.

NOTE: You do not need to make other configurations or start any services to configure this feature.

Tasks

- Adding SNMP servers
- Duplicating SNMP servers
- Editing SNMP servers
- Deleting an SNMP server
- Importing .MIB files

Adding SNMP servers

Use this task to add an SNMP server. To receive an SNMP trap, you must add the SNMP server's information so that ePolicy Orchestrator knows where to send the trap.

Task

For option definitions click **?** on the page displaying the options.

1 Go to **Automation | SNMP Servers**, then click **New SNMP Server** at the bottom of the page. the **New SNMP Server** page appears.

2 Provide the name and address of the SNMP server, then click **Save**.

The added SNMP Server appears in the **SNMP Servers** list.

Duplicating SNMP servers

Use this task to duplicate an existing SNMP server.

Task

For option definitions click **?** on the page displaying the options.

1 Go to **Automation | SNMP Servers**, then click **Duplicate** next to the desired SNMP server on which you want to base a new entry.

2 Provide a new name, then click **Save**.

The new SNMP server appears in the **SNMP Servers** list.

Editing SNMP servers

Use this task to edit existing SNMP server entries.

Task

For option definitions click **?** on the page displaying the options.

1 Go to **Automation | SNMP Servers**, then click **Edit** next to the desired SNMP server.

2 Edit the **Name** and **Address** information as needed, then click **Save**.

Deleting an SNMP server

Use this task to delete an SNMP server from Notifications.

Task

For option definitions click **?** on the page displaying the options.

1 Go to **Automation | SNMP Servers**, then click **Delete** next to the desired SNMP server.

2 When prompted, verify that you want to delete the SNMP server.

The SNMP Server is removed from the **SNMP Servers** list.

Importing .MIB files

Use this task to set up rules to send notification messages to an SNMP server via an SNMP trap. You must import the NAICOMPLETE.MIB file, located at:

\Program Files\McAfee\ePolicy Orchestrator\MIB

This file allows your network management program to decode the data in the SNMP traps into meaningful text.

For instructions on importing and implementing .MIB files, see the product documentation for your network management program.

Working with registered executables and external commands

Use these tasks to configure external commands by adding registered executables and assigning them to commands. You can configure notification rules to execute an external command when the rule is initiated.

Before you begin

Before configuring the list of external commands, place the registered executables at a location on the server where the rules can point.

Tasks

- Working with registered executables
- Working with external commands

Working with registered executables

Use these tasks to add, edit, and delete registered executables.

Before you begin

You must have appropriate permissions to perform these tasks.

You must use a browser session from the ePO server system.

Tasks

- Adding registered executables
- Editing registered executables
- Deleting registered executables

Adding registered executables

Use this task to add registered executables to your available resources. You can then configure commands and their arguments and assign them to your registered executables.

Before you begin

You must have appropriate permissions to perform this task.

You must use a browser session from the ePO server system.

Task

For option definitions, click **?** on the page displaying the options.

1. Go to **Automation | Registered Executables**, then click **New Registered Executable** at the bottom of the page. The **New Registered Executable** page appears.
2. Type a name for the registered executable.
3. Type the path or browse to and select the registered executable you want a rule to execute when triggered, then click **Save**.

The new registered executable appears in the **Registered Executables** list.

Editing registered executables

Use this task to edit an existing registered executable entry.

Before you begin

You must have appropriate permissions to perform this task.

You must use a browser session from the ePO server system.

Task

1 Go to **Automation | Registered Executables**, then select edit next to the desired executable in the list. The **Edit Registered Executable** page appears.

2 Edit the name or the select a diferent executable on the system, then click **Save**.

Deleting registered executables

Use this task to delete a registered executable entry.

Before you begin

- You must have appropriate permissions to perform this task.
- You must use a browser session from the ePO server system.

Task

1 Go to **Automation | Registered Executables**, then select **Delete** next to the desired executable in the list.

2 When prompted, click **OK**.

3 Click **OK**.

Working with external commands

Use these tasks to add, edit, and delete the external commands that launch registered executables when notification rules are triggered.

Tasks

- Adding external commands for use with registered executables
- Editing external commands
- Deleting external commands

Adding external commands for use with registered executables

Use this task to add commands, and configure their arguments, for existing registered executables.

Before you begin

You must have appropriate permissions to perform this task.

Task

For option definitions click **?** on the page displaying the options.

1. Go to **Automation | External Commands**, then click **New External Command** at the bottom of the page. The **New External Command** page appears.
2. Type the name of the command.
3. Select the desired **Registered Executable** to which you want to assign the command.
4. Type the desired **Arguments** for the command and insert any variables as needed, then click **Save**.

   NOTE: Transferring data output to a text file (piping) using extended characters (for example, | and >) is unsupported in **Arguments**, but can be accomplished by including it within a custom executable.

The new external command is added to the **External Commands** list.

Editing external commands

Use this task to edit an existing external command.

Before you begin

You must have appropriate permissions to perform this task.

Task

For option definitions click **?** on the page displaying the options.

1. Go to **Automation | External Commands**, then click **Edit** next to the desired command. The **Edit External Command** page appears.
2. Edit the name of the command, select a different registered executable, or change the arguments for the command.
3. Click **Save**.

Deleting external commands

Use this task to delete an existing external command.

Before you begin

You must have appropriate permissions to perform this task.

Task

For option definitions click **?** on the page displaying the options.

1. Go to **Automation | External Commands**, then click **Delete** next to the desired command..
2. When prompted, click **OK**.
3. Click **OK**.

Creating and editing Notification rules

Use these tasks to create and edit Notification rules. These allow you to define when, how, and to whom, notifications are sent.

NOTE: Notification rules do not have a dependency order.

Tasks

- Describing the rule
- Setting filters for the rule
- Setting thresholds of the rule
- Configuring the notifications for the rule

Describing the rule

Use this task to begin creating a rule. The **Description** page of the **Notification Rule Builder** wizard allows you to:

- Specify the System Tree group to which the rule applies.
- Name and describe the rule.
- Set a priority for the notification message (only when sent as email).
- Enable or disable the rule.

Task

For option definitions click **?** on the page displaying the options.

1 Go to **Automation | Notification Rules**, then click **New Rule**, or **Edit** next to an existing rule. The **Notification Rule Builder** wizard appears with the **Description** page displayed.

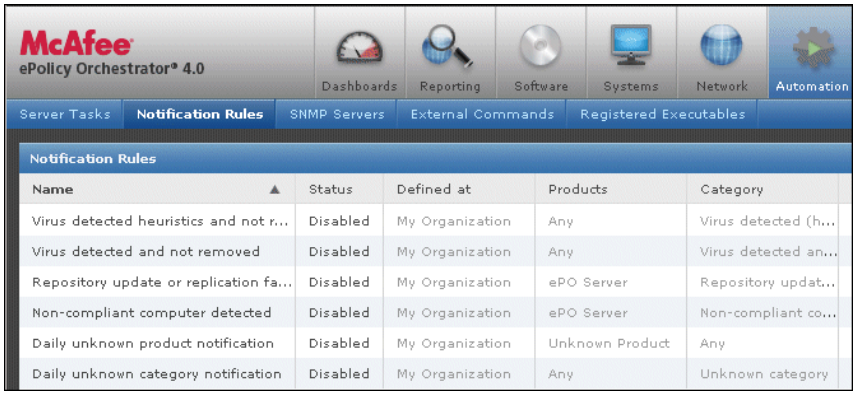

Figure 30: Notification Rules page

2 Type a unique name for the rule.

NOTE: Rule names on each server must be unique. For example, if one user creates a rule named **Emergency Alert**, no other user (including global administrators can create a rule with that name).

3 Type a description in the **Notes** text box.

4 Click **...** next to the **Defined at** text box, then select the desired System Tree group to which the rule applies from the **Select Tree Group** dialog box.

5 Set the priority of the rule to **High**, **Medium**, or **Low**.

NOTE: The priority of the rule is used to set a flag on an email message in the recipient's Inbox. For example, selecting **High** places a red exclamation mark next to the notification email message, and selecting **Low** places a blue, down-facing arrow next to the notification email message. The priority does not affect the rule or event processing in any way.

6 Select whether the rule is **Enabled** or **Disabled** next to **Status**.

7 Click **Next**.

Setting filters for the rule

Use this task to set the filters for the notification rule on the **Filters** page of the **Notification Rule Builder** wizard.

Task

For option definitions click **?** on the page displaying the options.

1 Select the types of **Operating systems** from which events can trigger the rule.

2 Select the **Products** whose events initiate this rule.

3 Select **Categories** of events that initiate this rule.

NOTE: Both the **Products** and **Categories** selections must be true to trigger the rule and send a notification message. For example, if you select **VirusScan** and **Virus detected but NOT cleaned**, the rule does not send a message for a Symantec Anti-Virus **Virus detected but NOT cleaned** event. If only the event category is important, then select **Any product**.

4 In **Threat name**, define the pattern matching the threat comparison to use:

a Select an operator from the drop-down list.

b Type any text for the operator to act on.

For example, use the name of a virus. Select **Contains** as the operator, then type **nimda** in the text box. This ensures that events are scanned for any line of text that contains **nimda**.

NOTE: If you select to filter on a threat name, the **Products**, **Categories**, *and* the **Threat name** selections must all be true for the rule to send a notification message.

5 Click **Next**.

Setting thresholds of the rule

Use this task to define when the rule triggers the rule on the **Thresholds** page of the **Notification Rule Builder** wizard.

A rule's thresholds are a combination of aggregation and throttling.

Task

For option definitions click **?** on the page displaying the options.

1 Next to **Aggregation**, select whether to **Send a notification for every event**, or to **Send a notification if multiple events occur within** a defined amount of time. If you select the latter, define this amount of time in minutes, hours, or days.

2 If you selected **Send a notification if multiple events occur within**, you can choose to send a notification when the specified conditions are met. These conditions are:

- **When the number of affected systems is at least** a defined number of systems.
- **When the number of events is at least** a defined number of events.
- Either (by selecting both options).

NOTE: You can select one or both options. For example, you can set the rule to send a notification if the number of affected systems exceeds 300, or when the number of events exceeds 3000, whichever threshold is crossed first.

3 If desired, next to **Throttling**, select **At most, send a notification every** and define an amount of time that must be passed before this rule can send notification messages again. The amount of time can be defined in minutes, hours, or days.

4 Click **Next**.

Configuring the notifications for the rule

Use this task to configure the notifications that are triggered by the rule on the **Notifications** page of the **Notification Rule Builder** wizard. These can be email messages, SNMP traps, or external commands. The size of the message depends on the target, the type of message, and the number of recipients of the message.

You can configure the rule to trigger multiple messages, SNMP traps, and external commands by using the **+** and **-** buttons next to the drop-down list for the type of notification.

Task

For option definition click **?** on the page displaying the options.

1 If you want the notification message to be sent as an email, or text pager message, select **Email Message** from the drop-down list.

a Next to **Recipients**, click **...** and select the recipients for the message. This list of available recipients is taken from Contacts (**Configuration | Contacts**). Alternatively, you can manually type email addresses separated by a comma.

b Type the **Subject** line of the message. Optionally, you can insert any of the available variables directly into the subject.

c Type any text you want to appear in the **Body** of the message. Optionally, you can insert any of the available variables directly into the body.

d Select the language in which you want the variables to appear from the **Replace variables with their values in** drop-down list.

e Click **Next** if finished, or click **+** to add another notification.

2 If you want the notification message to be sent as an SNMP trap, select **SNMP Trap** from the drop-down list.

a Select the desired **SNMP server** from the drop-down list.

b Select the desired language in which you want the variables to appear from the **Replace variables with their values in** drop-down list.

c Select the **Variables to include** in the SNMP trap.

- Notification rule name
- Rule defined at
- Rule group
- Selected products

- Selected categories
- First event time
- Event descriptions
- Actual number of events
- Actual categories
- Source systems
- Affected system names
- Affected objects
- Selected threat or rule name
- Event IDs
- Actual number of systems
- Actual products
- Actual threat or rule names
- Affected system IP addresses
- Time notification sent
- Additional information

NOTE: Some events do not include this information. If a selection you made is not represented, the information was not available in the event file.

d Click **Next** if finished, or click **+** to add another notification.

3 If you want the notification to be the execution of an external command:

a Select the desired external command from the **External command** drop-down list.

b Select the desired language in which you want the variables to appear from the **Replace variables with their values in** drop-down list.

c Click **Next** if finished, or click **+** to add another notification.

4 After clicking **Next**, the **Summary** page appears. Verify the information is correct, then click **Save**.

The new notification rule appears in the **Notification Rules** list.

Viewing the history of Notifications

Use these tasks to access and act on different types of information in the **Notification Log** page.

The Notifications Log page allows you to view the history of notifications sent. You can view a collective summary of all notifications sent, by product or category, or a list of all the specific notifications sent.

Tasks

- Configuring the Notification Log
- Viewing the details of Notification Log entries
- Purging the Notifications Log

Configuring the Notification Log

Use this task to configure and view a summary of the number of notifications sent by product, category, priority or rule name over a specified period of time for a specified location of the System Tree.

In this version of ePolicy Orchestrator, you can now display the information in the Notification Log as a summary table, pie chart, or bar chart.

Task

For option definitions, click **?** on the page displaying the options.

1. Go to **Reporting | Notification Log**.
2. Select the desired period of time for which you want to view notification history from the **Time filter** drop-down list.
3. Click **...** next to the **System Tree filter** text box. The **Select group to filter by** dialog box appears.
4. Select the desired group of the System Tree to view its notification history.

   NOTE: Users are limited to viewing only notifications history and rules for the parts of the System Tree to which they have permissions.

5. Select **Product**, **Category**, **Priority**, or **Rule name** from the **Group by** drop-down list. This selection determines how the log entries are organized when they are displayed.
6. Select **Summary Table**, **Pie Chart**, or **Bar Chart** from the **Display type** drop-down list. This selection determines the format in which the data is displayed. You can click the elements in any of these display types to drill down to the details of the item.
7. Use the **Sort by** drop-down list to display the items in a needed order.

Viewing the details of Notification Log entries

Use this task to view the details of notifications. This list can be sorted by the data of any column by clicking the column title.

Task

For option definitions, click **?** on the page displaying the options.

1. Configure the Notification Log as desired.
2. Click the desired summary table row, pie slice or bar of the display. A standard table appears displaying a list of all the notifications corresponding to the element of the primary display that was clicked.

   NOTE: Users are only able to view notifications for nodes of the System Tree to which they have permissions.

3. To sort the list, use the options from the **Sort by** drop-down list.
4. Click any notification in the table to view its details.

Purging the Notifications Log

Use this task to purge notifications from the Notifications Log. Notifications can be purged based on their age.

NOTE: When you purge items from the Notification Log, all entries are purged that meet the time criteria, regardless of which part of the System Tree they originated.

Before you begin

You must have permissions to perform this task.

Task

For option definitions, click **?** on the page displaying the options.

1. Go to **Reporting | Notification Log**, then click **Purge** at the bottom of the page. The Purge Notification Log dialog box appears.
2. Select the number of days, weeks, months, or years by which you want to purge all items of that age or older, or select a query to run that you have created for this purpose.

The Notification Log entries that meet this criteria are permanently deleted.

Product and component list

You can configure rules to generate notification messages for specific event categories of specific products and components. This is a list of products and components for which you can configure rules and a list of all possible event categories.

Supported products and components

- Desktop Firewall
- Host Intrusion Prevention
- ePO Server
- McAfee Agent
- GroupShield Domino
- GroupShield Exchange
- System Compliance Profiler
- Symantec NAV
- NetShield for NetWare
- PortalShield
- Stinger
- Unknown product
- Virex
- VirusScan Enterprise
- LinuxShield
- Security Shield

Frequently asked questions

If I set up a notification rule for virus detections, do I have to receive a notification message for each event received during an outbreak.

No. You can configure rules so that a notification can be sent only once per specified quantity of events within a specified amount of time, or sent at a maximum of once in a specified amount of time.

Can I create a rule that generates notifications to multiple recipients?

Yes. You can enter multiple email addresses for recipients in the **Notification Rule Builder** wizard.

Can I create a rule that generates multiple types of notifications?

Yes. Notifications for ePolicy Orchestrator supports any combination of the following notification targets for each rule:

- Email (including standard SMTP, SMS, and text pager).
- SNMP servers (via SNMP v1 traps).

- Any external tool installed on the ePolicy Orchestrator server.

Querying the Database

ePolicy Orchestrator 4.0.2 ships with its own querying and reporting capabilities. These are highly customizable and provide flexibility and ease of use. Included is the **Query Builder** wizard which creates and runs queries that result user-configured data in user-configured charts and tables.

To get you started, McAfee includes a set of default queries which provide the same information as the default reports of previous versions.

Are you setting up queries for the first time?

When setting up queries for the first time:

1. Understand the functionality of queries and the **Query Builder** wizard.
2. Review the default queries, and edit any to your needs.
3. Create queries for any needs that aren't met by the default queries.

Contents

- Queries
- Query Builder
- Multi-server roll-up querying
- Preparing for roll-up querying
- Working with queries
- Default queries and what they display

Queries

Queries are configurable objects that retrieve and display data from the database. The results of queries are displayed in charts and tables. Any query's results can be exported to a variety of formats, any of which can be dowloaded or sent as an attachment to an email message. Some queries can be used as dashboard monitors.

Query results are actionable

Query results are now actionable. Query results displayed in tables (and drill-down tables) have a variety of actions available for selected items in the table. For example, you can deploy agents to systems in a table of query results. Actions are available at the bottom of the results page.

Queries as dashboard monitors

Use almost any query (except those using a table to display the initial results) as a dashboard monitor. Dashboard monitors refresh automatically on a user-configured interval (five minutes by default).

Exported results

Query results can be exported to four different formats. Exported results are historical data and are not refreshed like when using queries as dashboard monitors. Like query results and query-based monitors displayed in the console, you can drill down into the HTML exports for more detailed information.

Unlike query results in the console, data in exported reports is not actionable.

Reports are available in several formats:

- CSV — Use this format to use the data in a spreadsheet application (for example, Microsoft Excel).
- XML — Use this format to transform the data for other purposes.
- HTML — Use this report format to view the exported results as a web page.
- PDF — Use this report format when you need to print the results.

Sharing queries between servers

Any query can be imported and exported, allowing you to share queries between servers. Any query needs to be created only once in a multi-server environment.

Public and personal queries

Queries can be personal or public. Private queries exist in the user's **My Queries** list, and are only available to their creator. Pubic queries exist in the **Public Queries** list, and are available to everyone who has permissions to use public queries.

Most default queries are only made available to the global administrator, who must make these default queries public for other users to access them. Several queries are public by default for use by the default dashboards.

Only users with appropriate permissions can make their personal queries public ones.

Query permissions

Use query permissions to assign specific levels of query functionality to permission sets, which are assigned to individual users.

Available permissions include:

- **No permissions** — The **Query** tab is unavailable to a user with no permissions.
- **Use public queries** — Grants permission to use any queries that have been created and made public by users with the same permissions.
- **Use public queries; create and edit personal queries** — Grants permission to use any queries that have been created and made public by users with the same permissions, as well as the ability to use the **Query Builder** wizard to create and edit personal queries.
- **Edit public queries; create and edit personal queries; make personal queries public** — Grants permission to use and edit any public queries, create and edit any personal queries,

as well as the ability to make any personal query available to anyone with access to public queries.

NOTE: To run some queries, you also need permissions to the feature sets associated with their result types. Also, in a query's results pages, the available actions to take on the resulting items depend on the feature sets a user has permission to.

Query Builder

ePolicy Orchestrator provides an easy, four-step wizard with which to create and edit custom queries. With the wizard you can configure which data is retrieved and displayed, and how it is displayed.

Result types

The first selection you make in the **Query Builder** wizard is a result type. This selection identifies what type of data the query will be retrieving. This selection determines what the available selections are in the rest of the wizard.

Result types include:

- Audit Log Entries — Retrieves information on changes and actions made by ePO users.
- Compliance History — Retrieves information on compliance counts over time. This query type and its results depend on a Run Query server task that generates compliance events from the results of a (Boolean pie chart) query. Additionally, when creating a Compliance History query, be sure the time unit matches the schedule interval for the server task. McAfee recommends creating the Boolean pie chart query first, followed by the server task that generates the compliance events, and finally the Compliance History query.
- Events — Retrieves information on events sent from managed systems.
- Managed Systems — Retrieves information about systems running the McAfee Security Agent.
- Notifications — Retrieves information on sent notifications.
- Repositories — Retrieves data on repositories and their status.
- Rolled-up Compliance History — Retrieves information on compliance counts over time from registered ePO servers. This query depends on server tasks being run on this ePO server and the registered servers.
- Rolled-up Managed Systems — Retrieves summary information on systems from registered ePO servers.

Chart types

ePolicy Orchestrator provides a number of charts and tables to display the data it retrieves. These and their drill-down tables are highly configurable.

NOTE: Tables do not include drill-down tables.

Chart types include:

- Bar chart
- Boolean pie chart
- Grouped bar chart

- Grouped summary table
- Line chart
- Pie chart
- Summary table
- Table

Table columns

Specify columns for the table. If you select **Table** as the primary display of the data, this configures that table. If you selected a type of chart as the primary display of data, this configures the drill-down table.

Query results displayed in a table are actionable. For example, if the table is populated with systems, you can deploy or wake up agents on those systems directly from the table.

Filters

Specify criteria by selecting properties and operators to limit the data retrieved by the query.

Multi-server roll-up querying

ePolicy Orchestrator 4.0.2 now includes the ability to run queries that report on summary data from multiple ePO databases. There are these result types in the Query Builder wizard that you can use for this type of querying:

- Rolled Up Managed Systems
- Rolled Up Compliance History

Query results from these types of queries are not actionable.

How it works

To roll up data for use by roll-up queries, you must register each server (including the local server) you want to include in the querying.

Once the servers are registered, then you must configure Data Roll Up server tasks on the reporting server (the server that performs the multi-server reporting). Data Roll Up server tasks retrieve the information from all databases involved in the reporting, and populates the eporollup_ tables on the reporting server.

The roll-up queries target these database tables on the reporting server.

NOTE: Use of the Rolled Up Compliance History type of query, requires an additional query (on Managed Systems with a Boolean pie chart) and an additional Run Query server task (with the subaction to generate a compliance event) to run on each server whose data you want to include in the Rolled Up Compliance History type of query.

Preparing for roll-up querying

Use these tasks to ensure the eporollup_ tables on the reporting server are populated and ready for using queries based on the Rolled Up query result types. These tasks should be performed for each server whose data will be included in the query results.

NOTE: Using the Rolled-Up Compliance History result type additionally requires that a Boolean pie chart-based query on managed systems be created on each server. Additionally, on each server, a Run Query server task needs to be created with a subaction to generate compliance events based on this query.

Tasks

- Registering ePO servers
- Creating a Data Roll Up server task

Registering ePO servers

Use this task to register each ePO server with the reporting server that you want to include in roll-up queries. You must also register the reporting server. Registering the servers ensures that summary data can be taken from each to populate the eporollup_ tables in the local database.

Task

For option definitions, click **?** on the page displaying the options.

1. Go to **Network | Registered Servers**, then click **New Server**. The **Registered Server Builder** wizard appears.
2. Select the server type and type a name and description, then click **Next**. The **Details** page appears.
3. Provide the details of the server, its database server, and the credentials to access the server, then click **Save**.

Creating a Data Roll Up server task

Use this task to create a Data Roll Up server task that populates the necessary tables on the reporting server with summary data from registered servers.

Best practices

McAfee recommends creating a Roll Up Data server task on this server for each registered servers. This task would include each of the desired Roll Up Data actions, each targeting only one of the registered servers.

Task

For option definitions, click **?** on the page displaying the options.

1. Go to **Automation | Server Tasks**, then click **New Task**. The **Server Task Builder** wizard appears.
2. Type a name and description for the task, and select whether to enable it, then click **Next**. The **Actions** page appears.

3 Select the desired Data Roll Up actions, and select the desired registered server to which it applies.

NOTE: McAfee recommends creating one server task per registered server, and configuring it to run both Roll Up Data actions.

4 Click **Next**. The **Schedule** page appears.

5 Schedule the task as needed, then click **Next**. The **Summary** page appears.

NOTE: If you are rolling up compliance history data, ensure that the time unit of the Roll-Up Compliance History query matches the schedule type of the Generate Compliance Event server tasks on the registered servers.

6 Review the settings, then click **Save**.

Working with queries

Use these tasks to create, use, and manage queries.

Tasks

- Creating custom queries
- Running an existing query
- Running a query on a schedule
- Making personal queries public
- Duplicating queries
- Sharing a query between ePO servers

Creating custom queries

Use this task to create custom queries with the Query Builder wizard. You can query on system properties, product properties, many of the log files, repositories, and more.

Task

For option definitions, click **?** on the page displaying the options.

1 Go to **Reporting | Queries**, then click **New Query**. The **Result Type** page of the **Query Builder** wizard appears.

2 Select the data type for this query. This choice determines the options available on subsequent pages of the wizard.

3 Click **Next**. The **Chart** page appears.

4 Select the type of chart or table to display the primary results of the query. Depending on the type of chart, there are different configuration options available.

5 Click **Next**. The **Columns** page appears.

6 Select the properties from the **Available Columns** list that you want as columns in the results table, then order them as desired with the arrow icons on the column headers.

NOTE: If you select **Table** on the **Chart** page, the columns you select here are the columns of that table. Otherwise, these are the columns of the drill-down table.

7 Click **Next**. The **Filter** page appears.

8 Select properties to narrow the search results. Selected properties appear in the content pane with operators to specify criteria to narrow the data that is returned for that property. Ensure your choices provide the data to display in the table columns configured in the previous step.

9 Click **Run**. The **Unsaved Query** page displays the results of the query, which is actionable, so you can take any available actions on items in any tables or drill-down tables.

- If this is a query you want to use again, click **Save** to add it to your **My Queries** list.
- If the query didn't appear to return the expected results, click **Edit Query** to go back to the **Query Builder** and edit the details of this query.
- If you don't need to save the query, click **Close**.

Running an existing query

Use this task to run an existing query from the **Queries** page.

Task

For option definitions, click **?** on the page displaying the options.

1 Go to **Reporting | Queries**, then select a query from the **Queries** list.

2 Click **Run**. The query results appear. Drill down into the report and take actions on items as necessary. Available actions depend on the permissions of the user.

3 Click **Close** when finished.

Running a query on a schedule

Use this task to create and schedule a server task that runs a query and takes actions on the query results.

Task

For option definitions, click **?** on the page displaying the options.

1 Go to **Automation | Server Tasks**, then click **New Task**. The **Description** page of the **Task Builder** wizard appears.

2 Name and describe the task, then click **Next**. The **Actions** page appears.

3 Select **Run Query** from the drop-down list.

4 Select the desired query to run.

5 Select the language in which to display the results.

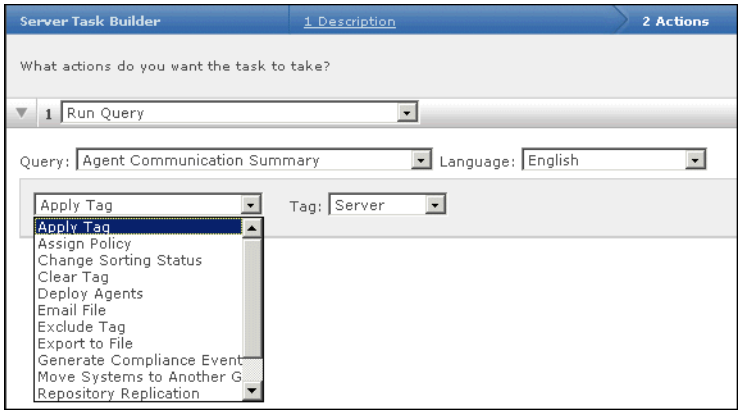

Figure 31: Run Query server task actions

6 Select an action to take on the results. Available actions depend on the permissions of the user, and include:

- **Email File** — Sends the results of the query to a specified recipient, in a user-configured format (PDF, XML, CSV, or HTML).
- **Move To** — Moves all systems in the query results to a group in the System Tree. This option is only valid for queries that result in a table of systems.
- **Change Sorting Status** — Enables or disables System Tree sorting on all systems in the query results. This option is only valid for queries that result in a table of systems.
- **Exclude Tag** — Excludes a specified tag from all systems in the query results. This option is only valid for queries that result in a table of systems.
- **Generate Compliance Event** — Generates an event based on a percentage or actual number threshold of systems that do not match the criteria in the query. This action is intended for compliance-based Boolean pie chart queries that retrieve data on managed systems (for example, the ePO: Compliance Summary default query). This action is part of the replacement of the Compliance Check server task of previous versions of ePolicy Orchestrator.
- **Repository Replication** — Replicates master repository contents to the distributed repositories in the query results. This is valuable for queries that return a list of out-of-date repositories (for example, the ePO: Distributed Repository Status default query). This option is only valid for queries that result in a table of distributed repositories.
- **Clear Tag** — Removes a specified tag from all systems in the query results. This option is only valid for queries that result in a table of systems.
- **Assign Policy** — Assigns a specified policy to all systems in the query results. This option is only valid for queries that result in a table of systems.
- **Export to File** — Exports the query results to a specified format. The exported file is placed in a location specified in the Printing and Exporting server settings.
- **Apply Tag** — Applies a specified tag to all systems (that are not excluded from the tag) in the query results. This option is only valid for queries that result in a table of systems.
- **Edit Description** — Overwrites the existing system description in the database for all systems in the query results. This option is only valid for queries that result in a table of systems.

- **Deploy Agents** — Deploys agents, according to the configuration on this page, to systems in the query results. This option is only valid for queries that result in a table of systems.
- **Wake Up Agents** — Sends an agent wake-up call, according to the configuration on this page, to all systems in the query results. This option is only valid for queries that result in a table of systems.

NOTE: You are not limited to selecting one action for the query results. Click the **+** button to add additional actions to take on the query results. Be careful to ensure you place the actions in the order you want them to be taken on the query results.

7 Click **Next**. The **Schedule** page appears.

8 Schedule the task as desired, then click **Next**. The **Summary** page appears.

9 Verify the configuration of the task, then click **Save**.

The task is added to the list on the **Server Tasks** page. If the task is enabled (by default), it runs at the next scheduled time. If the task is disabled, it only runs by clicking **Run** next to the task on the **Server Tasks** page.

Making personal queries public

Use this task to make personal queries public. All users with permissions to public queries have access to any personal queries you make public.

Before you begin

You must have appropriate permissions to perform this task.

Task

For option definitions, click **?** on the page displaying the options.

1 Go to **Reporting | Queries**, then select the desired query from the **My Queries** list.

2 Click **Make Public** at the bottom of the page.

NOTE: To access the **Make Public** action, you may need to click **More Actions**.

3 Click **OK** in the **Action** panel when prompted.

The query is added to the **Public Queries** list. All users that have access to public queries now have access to the query.

Duplicating queries

Use this task to create a query based on an existing query.

Task

For option definitions, click **?** on the page displaying the options.

1 Go to **Reporting | Queries**, then select the desired query from the **Queries** list.

2 Click **Duplicate**, provide a name for the duplicate, then click **OK**.

3 Select the new query in the **Queries** list, then click **Edit**. The **Query Builder** wizard appears with settings identical to those of the query that was the source for the duplicate.

4 Edit the query as desired, then click **Save**.

Sharing a query between ePO servers

Use these tasks to import and export a query for use among multiple servers.

Tasks

- Exporting queries for use by another ePO server
- Importing queries

Exporting queries for use by another ePO server

Use this task to export a query to an XML file which can be imported to another ePO server.

Task

For option definitions, click **?** on the page displaying the options.

1. Go to **Reporting | Queries**, then select a query from the **Queries** list.
2. Click **Export**, then **OK** in the **Action** panel. The **File Download** dialog box appears.
3. Click **Save**, select the desired location for the XML file, then click **OK**.

The file is saved in the specified location.

Importing queries

Use this task to import a query that was exported from another ePO server.

Task

For option definitions, click ? on the page displaying the options.

1. Go to **Reporting | Queries**, then click **Import Query**. The **Import Query** dialog box appears.
2. Click **Browse**. The **Choose File** dialog box appears.
3. Select the exported file, then click **OK**.
4. Click **OK**.

The query is added to the **My Queries** list.

Exporting query results to other formats

Use this task to export query results for other purposes. You can export to HTML and PDF finals for viewing formats, or to CSV or XML files for using and transforming the data in other applications.

Task

For option definitions, click **?** on the page displaying the options.

1. From the page displaying the query results, select **Export Table** or **Export Data** from the **Options** menu. The **Export** page appears.
2. Select whether the data files are exported individually or in a single archive (ZIP) file.
3. If needed, select whether to export the chart data only, or the chart data and drill-down tables.

4 Select the format of the exported file. If exporting to a PDF file, select the page size and orientation.

5 Select whether the files are emailed as attachments to selected recipients, or whether they are saved to a location on the server to which a link is provided. You can open or save the file to another location by right-clicking it.

   NOTE: When typing multiple email addresses for recipients, you must separate entries with a comma or semi-colon.

6 Click **Export**.

The files are created and either emailed as attachments to the recipients, or you are taken to a page where you can access the files from links.

Default queries and what they display

Use these queries for various purposes and tasks. This topic describes each of the default queries. Any product extensions installed may add their own default queries. Default query titles are introduced by the product acronym. (For example, VirusScan enterprise queries all begin with "VSE"). This section of the document covers McAfee Agent, and ePO queries only. See the product documentation of any others for information on their default queries.

MA: Agent Communication Summary query

Use this query, with its default settings, to view a Boolean pie chart of managed systems, divided according to whether agents have communicated with the server in the last day.

Query results

The results of the query are displayed in a Boolean pie chart, which you can use to drill down to systems that make up either pie slice.

Comparable report in ePolicy Orchestrator 3.6

This query replaces all or part of:

- Agent to Server Connection Info

MA: Agent Version Summary query

Use this query, with its default settings, to view a pie chart of managed systems, organized by the version of the agent they are running.

Query results

The results of the query are displayed in a pie chart, which you can use to drill down to a table of systems that make up each slice.

Comparable report in ePolicy Orchestrator 3.6

This query replaces all or part of:

- Agent Versions

ePO: Compliance History query

Use this query, with its default settings, to view the percentage of systems (over time) in your environment that are non-compliant.

Before you begin

This query and its results depend on the Generate Compliance Event server task. Schedule this server task to run at a regular interval. This query depends on a Boolean pie chart query based on managed systems (for example, the default ePO: Compliance Summary query).

Query results

The results of the query are displayed in a line chart. Details depend on the defined complaince of the ePO: Compliance Summary query.

Comparable report in ePolicy Orchestrator 3.6

This query replaces all or part of:

- DAT-Definition Deployment Summary
- DAT Engine Coverage

ePO: Compliance Summary query

Use this query, with its default settings, to show which managed systems in your environment are compliant or non-compliant by versions VirusScan Enterprise, McAfee Agent, and DAT files.

This query only considers systems that have communicated with the server in the last 24 hours.

Query results

The results of this query are displayed in a Boolean pie chart. One slice represents compliant systems, and the other represents non-compliant systems. The number of systems in each slice is displayed in the slice labels. You can drill down into either slice to an actionable table of systems.

Comparable report in ePolicy Orchestrator 3.6

This query replaces all or part of:

- DAT-Definition Deployment Summary
- DAT Engine Coverage

ePO: Malware Detection History query

Use this query, with its default settings, to view a line chart of the number of internal virus detections over the past quarter.

Query results

The results of the query are displayed in a line chart, which you can use to drill down into the details of the events and the systems on which they occurred.

Comparable report in ePolicy Orchestrator 3.6

This query replaces all or part of:

- DAT-Definition Deployment Summary
- DAT Engine Coverage

ePO: Distributed Repository Status query

Use this query, with its default settings, to view a Boolean pie chart of your distributed repositories, divided according to whether their last replication was successful.

Query results

The results of the query are displayed in a Boolean pie chart, which you can use to drill down to a table of repositories in that slice, which displays the name, type, and status of each.

ePO: Failed User Actions in ePO Console query

Use this query, with its default settings, to view a table of all failed actions from the Audit Log.

Query results

The results of the query are displayed in a table, which you can use to drill down into the details of the audited actions, events, and the systems on which they occurred.

ePO: Failed Logon Attempts query

Use this query, with its default settings, to view a Boolean pie chart of all logon attempts in the Audit Log, divided according to whether they were successful.

Query results

The results of the query are displayed in a Boolean pie chart, which you can use to drill down into the details of the events and the users for whom they occurred.

ePO: Multi-Server Compliance History query

Use this query, with its default settings, to view the percentage of systems that are non-compliant (over time) across registered servers.

Before you begin

This query and its results depend on the Data Rollup: Compliance History server task. Schedule the Data Rollup: Compliance History server task to run at a regular interval and be sure that the **Save results** checkbox is selected. Additionally, when creating a server task of this type, be sure the scedule type matches the time unit of this query. By default, this query's time unit matches the schedule type of the default Roll Up Data (Local ePO Server) server task.

Query results

This query returns a line chart. Details depend on how you've configured the Data Rollup: Compliance History server task.

Comparable report in ePolicy Orchestrator 3.6

This query replaces all or part of:

- DAT-Definition Deployment Summary
- DAT Engine Coverage

ePO: Systems per Top-Level Group query

Use this query, with its default settings, to view a bar chart of your managed systems organized by top-level System Tree group.

Query results

The results of the query are displayed in a bar chart, which you can use to drill down into the systems which make up each bar.

ePO: Systems Tagged as Server query

Use this query, with its default settings, to view a Boolean pie chart of the systems in your environment, divided according to whether they have the "Server" tag.

Query results

The results of the query are displayed in a Boolean pie chart, which you can use to drill down into the systems that make up each slice.

ePO: Today's Detections per Product query

Use this query, with its default settings, to view a pie chart of detections within the last 24 hours, organized by detecting product.

Query results

The results of the query are displayed in a pie chart, which you can use to drill down into the details of the events and the systems on which they occurred.

Comparable report in ePolicy Orchestrator 3.6

This query replaces all or part of:

- Number of Infections for the Past 24 Hours

Assessing Your Environment With Dashboards

Dashboards allow you to keep a constant eye on your environment. Dashboards are collections of monitors. Monitors can be anything from a chart-based query, to a small web application, like the MyAvert Security Threats, that is refreshed at a user-configured interval.

Users must have the appropriate permissions to use and create dashboards.

Are you setting up dashboards for the first time?

When setting up dashboards for the first time:

1. Review the conceptual topics in this section to better understand dashboards and dashboard monitors.
2. Decide which default dashboards and default monitors you want to use.
3. Create any needed dashboards and their monitors, and be sure to make active any you want available as tabs from the navigation bar.

Contents

- Dashboards and how they work
- Setting up dashboard access and behavior
- Working with Dashboards

Dashboards and how they work

Dashboards are collections of user-selected and configured monitors that provide current data about your environment.

Queries as dashboard monitors

Use any chart-based query as a dashboard that refreshes at a user-configured frequency, so you can use your most useful queries on a live dashboard.

Default dashboard monitors

This release of ePolicy Orchestrator ships with several default monitors:

- MyAvert Security Threats — Keeps you aware of which DATs and engines are available, what threats they protect, and the versions that are currently in your master repository.
- Quick System Search — A text-based search field that allows you to search for systems by system name, IP address, MAC address, or user name.

- McAfee Links — Hyperlinks to McAfee sites, including ePolicy Orchestrator Support, Avert Labs WebImmune, and Avert Labs Threat Library.

Setting up dashboard access and behavior

Use these tasks to ensure users have the appropriate access to dashboards, and how often dashboards are refreshed.

Tasks

- Giving users permissions to dashboards
- Configuring the refresh frequency of dashboards

Giving users permissions to dashboards

Use this task to give users the needed permissions to dashboards. For a user to be able to access or use dashboards, they must have the appropriate permissions.

Task

For option definitions, click **?** on the page displaying the options.

1. Go to **Configuration | Permission Sets**, then click **New Permission Set** or select a permission set in the **Permission Sets** list.
2. Next to **Dashboards**, click **Edit**. The **Edit Permission Set: Dashboards** page appears.
3. Select a permission:
   - **No permissions**
   - **Use public dashboards**
   - **Use public dashboards; create and edit personal dashboards**
   - **Edit public dashboards; create and edit personal dashboards; make personal dashboards public**
4. Click **Save**.

Configuring the refresh frequency of dashboards

Use this task to configure how often (in minutes) a user's dashboards are refreshed. This setting is unique to each user account.

When setting this, consider the number of users that you anticipate will be logged on at anytime. Each user logged on with a dashboard displayed creates additional performance usage when the dashboards are refreshed.

Task

For option definitions, click **?** on the page displaying the options.

1. Go to **Dashboards**, then select **Edit Dashboard Preferences** from the **Options** drop-down list. The **Dashboard Preferences** page appears.
2. Next to **Dashboard page refresh interval**, type the number of minutes you want between refreshes.
3. Click **Save**.

Working with Dashboards

Use these tasks to create and manage dashboards.

Tasks

- Creating dashboards
- Making a dashboard active
- Selecting all active dashboards
- Making a dashboard public

Creating dashboards

Use this task to create a dashboard.

Task

For option definitions, click **?** on the page displaying the options.

1 Go to **Dashboards**, then select **Manage Dashboards** from the **Options** drop-down list. The **Manage Dashboards** page appears.

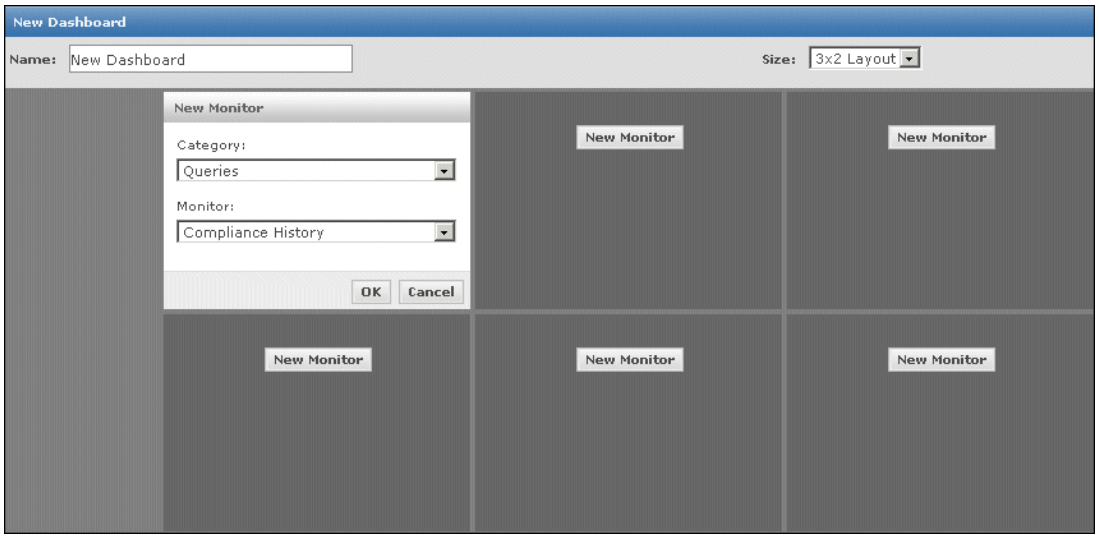

Figure 32: New Dashboard page

2 Click **New Dashboard**.

3 Type a name, and select a size for the dashboard.

4 For each monitor, click **New Monitor**, then select the monitor to display in the dashboard.

5 Click **Save**, then select whether to make this dashboard active. Active dashboards display on the tab bar of **Dashboards**.

Making a dashboard active

Use this task to make a dashboard part of your active set.

Task

For option definitions, click **?** on the page displaying them.

1 Go to **Dashboards**, click **Options**, then select **Manage Dashboards**. The **Manage Dashboards** page appears.

2 Select a dashboard from the **Dashboards** list, then click **Make Active**.

3 Click **OK** when prompted.

4 Click **Close**.

The selected dashboard is now on the tab bar.

Selecting all active dashboards

Use this task to select all dashboards that make up your active set. Active dashboards are accessible from on the tab bar under **Dashboards**.

Task

For option definitions, click **?** on the page displaying the options.

1 Go to **Dashboards**, then select **Select Active Dashboards** from the **Options** drop-down list.

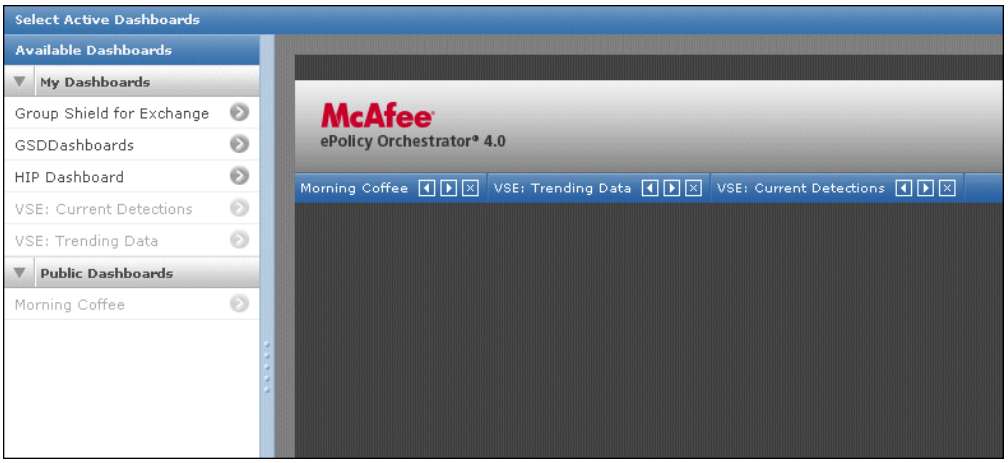

Figure 33: Select Active Dashboards page

2 Click the desired dashboards from the **Available Dashboards** list. They are added to the content pane.

3 Repeat until all desired dashboards are selected.

4 Arrange the selected dashboards in the order you want them to appear on the tab bar.

5 Click **OK**.

The selected dashboards appear on the tab bar whenever you go to the **Dashboards** section of the product.

Making a dashboard public

Use this task to make a private dashboard public. Public dashboards can be used by any user with permissions to public dashboards.

Task

For option definitions, click **?** on the page displaying the options.

1. Go to **Dashboards**, then select **Manage Dashboards** from the **Options** drop-down list.
2. Select the desired dashboard from the **Available Dashboards** list, then click **Make Public**.
3. Click **OK** when prompted.

The dashboard appears in the **Public Dashboards** list on the **Manage Dashboards** page.

Detecting Rogue Systems

Unprotected systems are often the weak spot of any security strategy, creating entry points through which viruses and other potentially harmful programs can access your network. Even in a managed network environment, some systems might not have an active McAfee Agent on them. These can be systems that frequently log on and off the network, including test servers, laptops, or wireless devices.

Rogue System Detection provides real-time detection of rogue systems through use of the Rogue System Sensor installed throughout your network. The sensor listens to network broadcast messages and DHCP responses to detect systems connected to the network.

When a sensor detects a system on the network, it sends a message to the ePolicy Orchestrator server. The server then checks whether the system has an active agent installed and managed. If the system is unknown to the ePO server, Rogue System Detection provides information to ePolicy Orchestrator to allow you to take remediation steps, including alerting network and anti-virus administrators or automatically deploying an agent to the system.

Contents

- What are rogue systems
- How the Rogue System Sensor works
- How detected systems are matched and merged
- Rogue System Detection states
- Rogue Sensor Blacklist
- Rogue System Detection policy settings
- Rogue System Detection permission sets
- Setting up Rogue System Detection
- Configuring Rogue System Detection policy settings
- Configuring server settings for Rogue System Detection
- Setting up automatic responses to Rogue System Detection events
- Working with detected systems
- Working with sensors
- Working with subnets
- Rogue System Detection command-line options
- Default Rogue System Detection queries

What are rogue systems

Rogue systems are systems that access your network, but are not managed by your ePO server. A rogue system can be any device on your network that has a network interface card (NIC).

On systems that have multiple NICs, each resulting interface can be detected as a separate system. When these interfaces are detected, they can appear as multiple rogue interfaces.

Identifying these systems and their interfaces, and managing them with Rogue System Detection and ePolicy Orchestrator helps provide the network security your organization needs.

How the Rogue System Sensor works

The Rogue System Sensor is the distributed portion of the Rogue System Detection architecture. Sensors detect systems, routers, printers, and other devices connected to your network. They gather information about devices they detect, and forward the information to the ePO server.

The sensor is a Win32 native executable application that runs on any NT-based Windows operating system, such as Windows 2000, Windows XP, or Windows Server 2003. It can be installed on systems throughout your network. A sensor reports on all systems in the broadcast segment where it is installed. A sensor installed on a DHCP server reports on all systems or subnets using DHCP. In networks or broadcast segments that don't use DHCP servers, you must install at least one sensor in each broadcast segment, usually the same as a subnet, to maintain coverage. DHCP deployment can be used in conjunction with segment-specific deployment for the most comprehensive coverage.

Passive listening to layer-2 traffic

To detect systems on the network, the sensor uses WinPCap, a packet capture library. It captures layer-2 broadcast packets sent by systems connected to the same network broadcast segment and listens passively to all layer-2 traffic for Address Resolution Protocol (ARP), Reverse Address Resolution Protocol (RARP), IP traffic, and DHCP responses.

The sensor also performs NetBIOS calls and OS fingerprinting on systems already detected to obtain additional information. It does this by listening to the broadcast traffic of all devices in its broadcast segment and by using NetBIOS calls to actively probe the network to gather additional information about the devices connected to it, such as detected system operating system.

NOTE: The sensor does not determine whether the system is a rogue system. It detects systems connected to the network and reports these detections back to the ePO server.

Intelligent filtering of network traffic

The sensor implements intelligent filtering of network traffic: it ignores unnecessary messages and captures only what it needs, Ethernet and IP broadcast traffic. By filtering out unicast traffic (DHCP monitoring uses unicast traffic, but only looks at DCHCP responses), which might contain non-local IP addresses, the sensor focuses only on devices that are part of the local network.

To optimize performance and minimize network traffic, the sensor limits its communication to the server by relaying only new system detections, and by ignoring any re-detected systems for a user-configured time. For example, the sensor detects itself among the list of detected systems. If the sensor sent a message every time it detected a packet from itself, the result would be a network overloaded with sensor detection messages.

The sensor further filters on systems already detected:

- The sensor reports any system the first time it is detected on the network.
- For each detected system, the sensor adds the MAC address to the packet filter, so that it is not detected again, until the user configured time elapses.

- The sensor implements aging on the MAC filter. After a specified time, MAC addresses for systems that have already been detected are removed from the filter, causing those systems to be re-detected and reported to the server. This process ensures that you receive accurate and current information about detected systems.

Data gathering and communications to the server

Once the sensor detects a system on the local network, it gathers information about that system from the data contained in the network packet. This information includes:

- DNS name.
- Operating system version.
- NetBIOS information (domain membership, system name, and the list of currently logged-on users).

All of the NetBIOS-related information gathered is subject to standard limitations of authorization and other limitations, as documented in the Microsoft management API.

The sensor packages the gathered information into an XML message, then sends the message via secure HTTPS to the ePolicy Orchestrator server for processing. The server then uses the ePolicy Orchestrator data to determine whether the system is a rogue system.

Bandwidth use and sensor configuration

To save bandwidth in large deployments, you can configure how often the sensor sends detection messages to the server. You can configure the sensor to cache detection events for a given time period, such as one hour, then to send a single message containing all the events from that time period. For more information, see *Configuring Rogue System Detection policy settings*.

Systems that host sensors

Install sensors on systems that are likely to remain on and connected to the network at all times, such as servers. If you don't have a server running in a given broadcast segment, install sensors on several workstations to ensure that at least one sensor is connected to the network at all times.

TIP: To guarantee that your Rogue System Detection coverage is complete, you must install at least one sensor in each broadcast segment of your network. Installing more than one sensor in a broadcast segment does not create issues around duplicate messages because the server filters any duplicates. However, additional active sensors in each subnet results in traffic sent from each sensor to the server. While maintaining as many as five or ten sensors in a broadcast segment should not cause any bandwidth issues, you should not maintain more sensors in a broadcast segment than is necessary to guarantee coverage.

DHCP servers

If you use DHCP servers in your network, you can install sensors on them. Sensors installed on DHCP servers (or spanned ports on DHCP servers) report on all subnets connected to it by listening for DHCP responses. Using sensors on DHCP servers reduces the number of sensors you need to install and manage on your network to ensure coverage, but it does not eliminate the need to install sensors to systems that use static IP address.

TIP: Installing sensors on DHCP servers can improve coverage of your network. However, it is still necessary to install sensors in broadcast segments that use static IP address, or that have

a mixed environment. A sensor installed on a DHCP server will not report on systems covered by that server if the system uses a static IP address.

How detected systems are matched and merged

When a system connects to your network, Rogue System Detection automatically checks the ePO database to determine whether the incoming system is new or corresponds to a previously detected system. If the system has been previously detected, Rogue System Detection matches it to the existing record in the ePO database automatically. When a detected system is not matched automatically, you can manually merge the system with an existing detected system.

Matching detected systems

Automatic matching of detected systems is necessary to prevent previously detected systems from being identified as new systems on your network. By default, systems are first matched against an agent's unique ID. If this unique ID does not exist, the ePO database uses attributes specified in the Rogue System Matching server settings. You can specify which attributes the database uses for matching, based on which attributes are unique in your environment.

If a system on your network has multiple NICs, each system interface can result in separate detections. You can specify how the system interfaces are matched in the same manner used for specifying the matching of detected systems.

Merging detected systems

When the ePO server cannot automatically match detected systems, you can merge them manually. For example, the ePO server might not be able to match a detected system interface generated by a system with multiple NICs based on the matching attributes you have specified. For more information, see *Merging detected systems*.

Rogue System Detection states

Rogue System Detection categorizes systems, sensors and subnets on your network with different states to make monitoring and managing your network easier. These states determine the following:

- Overall system status
- Rogue System Sensor status
- Subnet status

The Detected Systems homepage displays information on each of these states via corresponding status monitors. This page also displays the 25 subnets with the most rogue system interfaces in the Top 25 Subnets list and the adjacent Rogue System Interfaces by Subnet table.

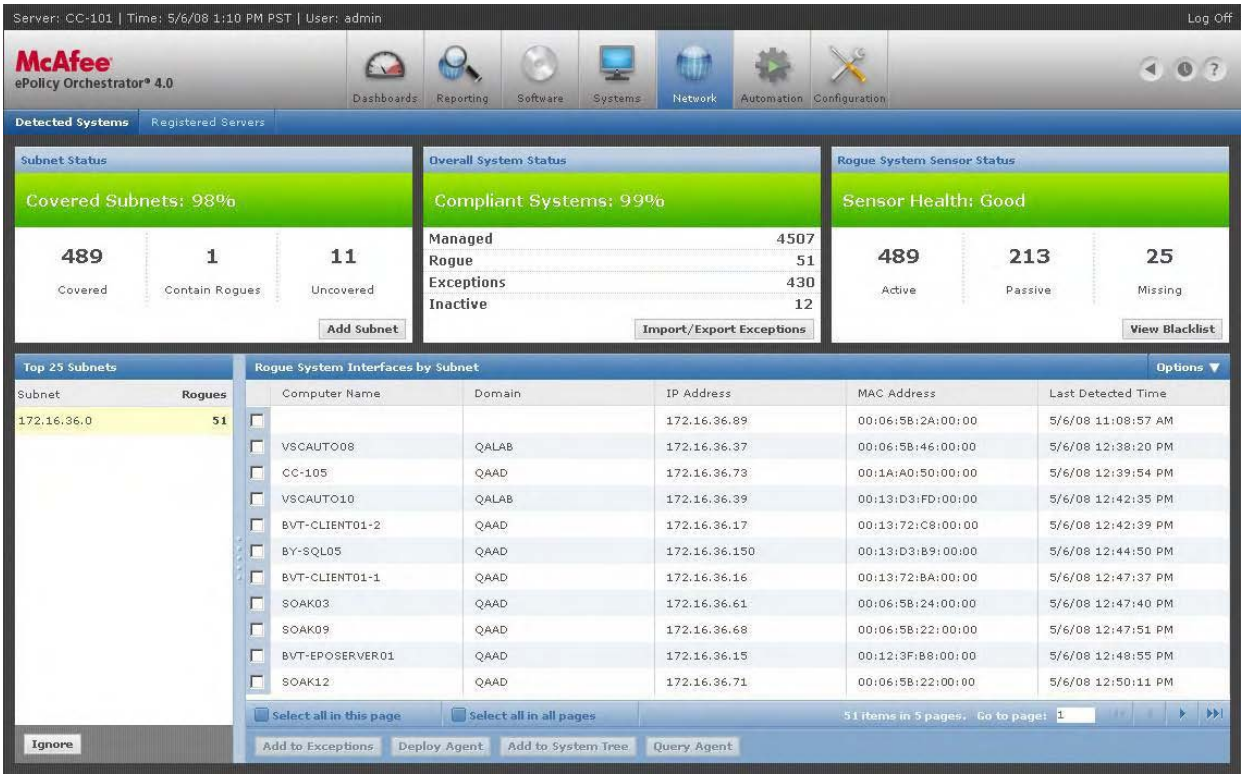

Figure 34: Detected Systems homepage

Overall system status

Overall system status is presented in the Overall System Status monitor as a percentage of compliant systems. Systems states are separated into these categories:

- Exceptions
- Inactive
- Managed
- Rogue

The percentage of compliant systems is the ratio of systems in the Managed and Exceptions categories to those in the Rogue and Inactive categories.

Exceptions

Exceptions are systems that don't need a McAfee Agent, such as routers, printers, or systems from which you no longer want to receive detection information. Identify these systems and mark them as exceptions to prevent them from being categorized as rogue systems. Mark a system as an exception only when it does not represent a vulnerability in your environment.

Inactive

Inactive systems are listed in the ePO database, but have not been detected by a Rogue System Sensor in a specified time, which exceeds the period specified in the Rogue category. These

are most likely systems that are shut down or disconnected from the network, for example, a laptop or retired system. The default time period for marking systems as inactive is 45 days.

Managed

Managed systems have an active McAfee Agent that has communicated with the ePO server in a specified time. The majority of detected systems on your network should be managed to ensure security.

NOTE: Systems on your network that have an active agent installed are displayed in this list, even before you deploy sensors to the subnets that contain these systems. When the agent reports to the ePO database, the system is automatically listed in the Managed category.

Rogue

Rogue systems are systems that are not managed by your ePO server. There are three rogue states:

- Alien agent — These systems have a McAfee Agent that is not in the local ePO database.
- Inactive agent — These systems have a McAfee Agent in the ePO database that has not communicated in a specified time.
- Rogue — These systems don't have a McAfee Agent.

Systems in any of these three rogue states are categorized as Rogue systems.

Rogue System Sensor status

Rogue System Sensor status is the measure of how many sensors installed on your network are actively reporting to the ePO server, and is displayed in terms of health. Health is determined by the ratio of active sensors to missing sensors on your network. Sensor states are categorized into these groups:

- Active
- Missing
- Passive

Active

Active sensors report information about their broadcast segment to the ePO server at regular intervals, over a fixed time. Both the reporting period and the active period are user-configured. A sensor becomes passive when the active period lapses, at which time the next passive sensor to report in is made active.

Missing

Missing sensors have not communicated with the ePO server in a user-configured time. These sensors could be on a system that has been turned off or removed from the network.

Passive

Passive sensors check in with the ePO server, but do not report information about detected systems. They wait for instructions from the ePO server to replace other sensors that become passive.

Subnet status

Subnet status is the measure of how many detected subnets on your network are covered. Coverage is determined by the ratio of covered subnets to uncovered subnets on your network. Subnet states are categorized into these groups:

- Contains Rogues
- Covered
- Uncovered

NOTE: Subnets must be known by the ePO server or be seen by a sensor to fall into one of these categories.

Contains Rogues

Subnets that contain rogue systems are listed in the Contains Rogues category to make it easier to take action on them.

Covered

Covered subnets have sensors installed on them that are actively reporting information to the ePO server about detected systems. The Covered subnets category also includes the systems listed in the Contains Rogues category. For example, the Covered subnets category contains subnets A, B, and C. Subnet B contains rogues, while A and C do not. All three are listed in the Covered category; only subnet B is listed in the Contains Rogues category.

Uncovered

Uncovered subnets don't have any active sensors on them. Subnets that are uncovered are not reporting information about detected systems to the ePO server.

Top 25 Subnets

The Top 25 Subnets list provides the starting IP addresses and subnet range for the 25 subnets that contain the most rogue system interfaces on your network. When a top 25 subnet is selected, the rogue system interfaces it contains are displayed in the adjacent Rogue System Interfaces by Subnet table.

Rogue Sensor Blacklist

The Rogue Sensor Blacklist is the list of managed systems where you do not want sensors installed. These can include systems that would be adversely affected if a sensor were installed on them, or systems you have otherwise determined should not host sensors. For example, mission critical servers where peak performance of core services is essential, such as database servers or servers in the DMZ (demilitarized zone). Also, systems that might spend significant time outside your network, such as laptops.

The Rogue Sensor Blacklist is different than the Exceptions list, in that systems on the Exceptions list are those that either can't have an agent on them, or that you don't want categorized as Rogue, such as printers or routers.

Rogue System Detection policy settings

Rogue System Detection policy settings allow you to configure and manage the instances of the Rogue System Sensor installed throughout your network. Settings can be applied to individual systems, groups of systems, and subnets.

You can configure policy settings for all sensors deployed by the server. This is similar to managing policies for any deployed product, such as VirusScan Enterprise. The Rogue System Detection policy pages are installed on the ePO server at installation.

Configure the sensor policy settings in the Rogue System Detection policy pages the same way you would for any managed security product. Policy settings you assign to higher levels of the System Tree are inherited by lower-level groups or individual systems. For more information about policies and how they work, see *Managing Products with Policies and Client Tasks*.

TIP: McAfee recommends that you configure policy settings before you deploy sensors to your network. Doing so ensures that the sensors work according to your intended use. For example, DHCP monitoring is disabled by default. As a result, if you deploy sensors to DHCP servers without enabling DHCP monitoring during your initial configuration, those sensors report limited information to the ePO server. If you deploy sensors before you configure your policies, you can update them to change sensor functionality.

Considerations for policy settings

Policy settings configure the features and performance of the Rogue System Sensor. These settings are separated into four groups:

- Communication settings
- Detection settings
- General settings
- Interface settings

Communication settings

Communication settings determine:

- The communication time for inactive sensors.
- The reporting time for active sensors.
- The sensor's detected system cache lifetime.

The sensor's detected system cache lifetime is the amount of time a detected system remains in the sensor's cache. This value controls how often the sensor reports that a system is newly detected. The lower the value, the more often the sensor reports a system detection to the server. Setting this value too low can overwhelm your server with system detections. Setting this value too high prevents you from having current information on system detections.

The communication time for inactive sensors determines how often passive sensors check in with the server. If a sensor fails to check in during this time period, it is marked as missing.

The Reporting time for active sensors determines how often active sensors report to the ePO server. Setting this value too high or low can have the same effect as setting the value for the sensor's detected system cache lifetime.

TIP: McAfee recommends that you set the sensor's detected system cache lifetime and the reporting time for active sensors settings to the same value.

Detection settings

Detection settings determine whether:

- Active Probing is enabled.
- DHCP monitoring is enabled.

If you use DHCP servers on your network, you can install sensors on them to monitor your network. This allows you to use a single sensor to report on all subnets and systems that connect to it. DHCP monitoring allows you to cover your network with fewer sensors to deploy and manage, and reduces the potential for missed subnets and systems.

Active probing uses NetBIOS calls to provide more detailed information about the devices on your network. You can enable active probing on your entire network, or include or exclude specific subnets.

CAUTION: This feature provides accurate matching of detected system interfaces and should be disabled only if you have specific reasons to do so.

General settings

General settings determine:

- The sensor-to-server communication port.
- The server IP address or DNS name.
- Whether the Rogue System Sensor is enabled.

The server IP address default value is the address of the ePO server that you are using to install sensors. Rogue System Detection reports system detections to the specified server. When this server detects a system that has an agent deployed by an ePO server with a different IP address, that system is detected as a rogue because the agent is considered an alien agent.

Interface settings

Interface settings determine whether sensors:

- Do not listen on interfaces whose IP addresses are included in specific networks.
- Only listen on an interface if its IP address is included on a network found during installation.
- Only listen on interfaces whose IP addresses are included in specific networks.

Specifying these settings allows you to choose the networks that the sensor reports on.

Rogue System Detection permission sets

Permission sets for Rogue System Detection determine what information a user group can view, modify or create for Rogue System Detection. One or more permission sets can be assigned. By default, permission sets for global administrators are automatically assigned to include full access to all products and features.

The permission sets and their available privileges for Rogue System Detection are listed in the following table.

Permission set	Rights
Rogue System Detection	• Create and edit Rogue System information; manage sensors. • Create and edit Rogue System information; manage sensors; Deploy McAfee Agents and Add to System Tree. • No permissions.

Permission set	Rights
	• View Rogue System information.
Rogue System Sensor	• No permissions. • View and change settings. • View settings.

Setting up Rogue System Detection

Use these tasks to set up Rogue System Detection.

Protecting your network requires accurate information about the systems that connect to it. Rogue System Detection uses sensors to monitor the detected systems on your network to provide this information.

Before you begin

Before you begin setting up Rogue System Detection:

- Make sure you have agents distributed to your systems. For more information, see *Distributing agents*.
- Review the information in the preceding sections to understand the sensor and its policies.

Tasks

- Configuring Rogue System Detection policy settings
- Configuring server settings for Rogue System Detection
- Setting up automatic responses to Rogue System Detection events

Configuring Rogue System Detection policy settings

Use this task to configure Rogue System Detection policy settings. Policy settings determine how the sensor obtains and reports information about system detected on your network.

Task

For option definitions, click **?** on the page displaying the options.

1. Go to **Systems | Policy Catalog**, then from the **Product** drop-down list select **Rogue System Detection 2.0.0**, and from the **Category** drop-down list select **General**. All created policies for Rogue System Detection appear.
2. Edit an existing policy, or create a new policy.
   - To edit an existing policy, locate the desired policy and click **Edit** in its row.
   - To create a new policy, click **New Policy** and, from the **Create a policy based on this existing policy** drop-down list, select an existing policy on which to base the new policy. Name the new policy and click **OK**.
3. Configure the desired settings and click **Save**.

Configuring server settings for Rogue System Detection

Use these tasks to configure server settings for Rogue System Detection. These settings determine how information about subnets and detected systems is displayed in the **Detected Systems** homepage. Server settings allow you to customize Rogue System Detection to meet the specific needs of your organization.

Tasks

- Editing compliance settings
- Editing matching settings
- Editing sensor settings

Editing compliance settings

Use this task to edit the Rogue System Compliance settings. These settings are user-configured and have two important functions:

- They specify the time-frames that determine the state of detected systems (**Managed, Rogue, Exception, Inactive**).
- They control the visual feedback of the Rogue System Detection status monitors on the **Detected Systems** homepage.

Task

For option definitions, click **?** on the page displaying the options.

1. Go to **Configuration | Server Settings**, then in the **Settings Categories** list click **Rogue System Compliance**.
2. In the details pane click **Edit**.
3. Edit the number of days to categorize **Detected Systems** as **Managed** or **Inactive**.

   NOTE: The number of days in **Rogue | Has Agent in ePO Database, but is older than__ days** is controlled by the number of days set in the **Managed** field.

4. Edit the percentage levels for these options, so that the color codes represent your requirements:
   - **Covered Subnets** — required coverage.
   - **System Compliance** — required compliance status.
   - **Sensor Health** — ratio of active to missing sensors.
5. Click **Save**.

Editing matching settings

Use this task to edit the matching settings for Rogue System Detection. Matching settings are user-configured and have these important functions:

- They define the properties that determine how newly detected interfaces are matched with existing systems.
- They specify static IP ranges for matching.

- They specify which ports to check for a McAfee Agent.

Task

For option definitions, click **?** on the page displaying the options.

1. Go to **Configuration | Server Settings**, then in the **Settings Categories** list click **Rogue System Matching**.
2. Click **Edit**.
3. Use the **Matching Detected Systems** table to define the properties that determine when to match or merge detected systems.
4. Use the **Matching Managed Systems** table to define the properties that determine when a newly detected interface belongs to an existing detected system.
5. In **Static IP Ranges for Matching**, type the static IP ranges to use when matching on static IP addresses.
6. In **Alternative McAfee Agent Ports**, specify any alternate ports you want to use when querying detected systems to check for a McAfee Agent.
7. Click **Save**.

Editing sensor settings

Use this task to edit the sensor settings for Rogue System Detection. Sensor settings are user-configured and specify:

- The amount of time sensors are active.
- The maximum number of sensors active in each subnet.
- How long the server waits to hear from a sensor before categorizing it as missing.

Task

For option definitions, click **?** on the page displaying the options.

1. Go to **Configuration | Server Settings**, then in the **Settings Categories** list click **Rogue System Sensor**.
2. Click **Edit**.
3. Edit the **Sensor Timeout** minutes field to set the maximum number of minutes the server waits for a sensor to call in before marking it as missing.
4. Edit the **Sensors per Subnet** field to set the maximum number of sensors active in each subnet.
5. Edit the **Active Period** minutes field to set the maximum amount of time that passes before the server tells a sensor to sleep, to allow a new sensor to become active.
6. Click **Save**.

Setting up automatic responses to Rogue System Detection events

Use this task to set up automatic responses to Rogue System Detection events using the **Response Builder** wizard. You can configure Rogue System Detection to generate an automatic response when:

- A system is added to the **Exceptions** list.
- A system is detected.
- A subnet falls into the uncovered state.

Task

For option definitions, click **?** on the page displaying the options.

1 Go to **Automation** | **Responses** and click **New Response**. The **Response Builder** wizard opens.

2 In the **Description** page:

a Type a name for the new response, and any notes.

b From the **Event group** drop-down list, select **Rogue System Events**.

c From the **Event type** drop-down list, select an event type.

Table 2: Event type option definitions

Option	Definition
Add to Exceptions	Triggers a response any time a system is added to the Exceptions list.
Subnet Falls Into Uncovered State	Triggers a response any time a subnet does not have any active sensors monitoring it.
Rogue System Detected	Triggers a response any time a rogue system is detected.

d Select **Enabled** to activate the response, then click **Next**.

3 On the **Filter** page from the **Available Properties** list, click the properties you want to use to filter events, then click **Next**.

4 In the **Aggregation** page, specify how you want events to be aggregated, the click **Next**.

5 In the **Actions** page, select the action to perform when this response is triggered, then click **Next**.

Table 3: Action results

Action	Result
Add to Exceptions	Adds the detected system to the Exceptions list.
Add to System Tree	Adds the detected system to the System Tree.
Delete Detected System	Removes the detected system associated with this event.
Deploy Agent	Deploys a McAfee Agent to the detected system.
Query Agent	Opens the Query McAfee Agent Results page, which provides the name of IP address of the detected system and details about the agent installed on it.
Remove from Exceptions	Removes the detected system from the Exceptions list.

Action	Result
Send Email	Sends an email to user-configured recipients with a customized subject and message.

6 In the **Summary** page review the response details, then click **Save**.

Working with detected systems

Use these tasks to manage detected systems in Rogue System Detection.

Tasks

- Adding systems to the Exceptions list
- Adding systems to the Rogue Sensor Blacklist
- Editing system comments
- Exporting the Exceptions list
- Importing systems to the Exceptions list
- Merging detected systems
- Removing systems from the Detected Systems list
- Removing systems from the Exceptions list
- Removing systems from the Rogue Sensor Blacklist
- Viewing detected systems and their details

Adding systems to the Exceptions list

Use this task to add detected systems to the **Exceptions** list.

This task can be performed from:	Getting there
Detected Systems Details page.	Go to **Network | Detected Systems**, click any detected system category in the **Overall System Status** monitor, and click any system.
Detected Systems homepage.	Go to **Network | Detected Systems**.
Detected Systems page.	Go to **Network | Detected Systems** and click any detected system category in the **Overall System Status** monitor.

Task

For option definitions, click **?** on the page displaying the options.

1 Select the detected systems you want to add to the **Exceptions** list.

NOTE: From the **Detected Systems Details** page, you can only add the detected system you are viewing.

2 Click **Add to Exceptions**.

Adding systems to the Rogue Sensor Blacklist

Use this task to add detected systems to the **Rogue Sensor Blacklist**.

This task can be performed from:	Getting there
Managed Systems for Subnet xxx.xxx.xxx.xxx page.	Go to **Network | Detected Systems**, click any subnet category in the **Subnet Status** monitor, then select any subnet and click **View Managed Systems.**
Systems Details page.	Go to **Systems | System Tree | Systems** and click any system.
Systems page.	Go to **Systems | System Tree**.

Task

For option definitions, click **?** on the page displaying the options.

1 Select the detected systems you want to add to the **Rogue Sensor Blacklist**.
From the **Systems Details** page, you can only add the detected system you are viewing.

2 Click **Rogue Sensor Blacklist Add**.

NOTE: If the **Rogue Sensor Blacklist Add** button is not visible, click **More Actions** and select **Rogue Sensor Blacklist Add**.

Editing system comments

Use this task to edit system comments. System comments can be useful for noting important "human readable" information to a detected system entry.

This task can be performed from:	Getting there
Detected Systems Details page.	Go to **Network | Detected Systems**, click any detected system category in the **Overall System Status** monitor, and click any system.
Detected Systems page.	Go to **Network | Detected Systems** and click any detected system category in the **Overall System Status** monitor.

Task

For option definitions, click **?** on the page displaying the options.

1 Select the system whose comment you want to edit, and click **Edit Comment**.

2 In the **Action** pane, type the new comment for the system, then click **OK**.

Exporting the Exceptions list

Use this task to export the list of detected systems on your network marked as **Exceptions**.

Task

For option definitions, click **?** on the page displaying the options.

1 Go to **Network | Detected Systems** and click **Import/Export Exceptions**, then click the **Export** tab.

2 Click **Export**.

NOTE: Files are exported in the Comma Separated Value format. The file name for your **Exceptions** list is predefined as **RSDExportedExceptions.csv**. You can change the name of the file after it has been exported to your local system.

Importing systems to the Exceptions list

Use this task to import systems to your network's **Exceptions** list.

Task

For option definitions, click **?** on the page displaying the options.

1. Go to **Network | Detected Systems** and click **Import/Export Exceptions**, then click the **Import** tab.
2. Choose the method you want to use to import and specify the systems or file, then click **Import**.

   NOTE: When importing systems by name, MAC addresses can be separated by whitespace, commas, or semicolons. The MAC address can include colons, but they are not required.

Merging detected systems

Use this task to merge detected systems.

Task

For option definitions, click **?** on the page displaying the options.

1. From the **Detected Systems** page, select the detected systems (or system interfaces) you want to merge.
2. Click **Merge Systems**. The **Merge Systems** page appears.
3. Click **Merge**.

Removing systems from the Detected Systems list

Use this task to remove systems from the **Detected Systems**. For example, you might want to remove systems from the Detected Systems list when you know it is no longer in service. Once a system has been removed, it will not appear in the Detected Systems list until the next time the Rogue System Sensor detects it, or you manually add it back to the list.

This task can be performed from:	Getting there
Detected Systems Details page.	Go to **Network	Detected Systems,** click any detected system category in the **Overall System Status** monitor, and click any system.
Detected Systems page.	Go to **Network	Detected Systems** and click any detected system category in the **Overall System Status** monitor.
Managed Systems for Subnet xxx.xxx.xxx.xxx page.	Go to **Network	Detected Systems**, click any subnet category in the **Subnet Status** monitor, then select any subnet and click **View Managed Systems.**
Systems Details page.	Go to **Systems	System Tree	Systems** and click any system.
Systems page.	Go to **Systems	System Tree**.

Task

For option definitions, click **?** on the page displaying the options.

1 Select the systems you want to remove from the **Detected Systems** list.
From the **Systems Details** page and the **Detected Systems Details** page, you can only delete the detected system you are viewing.
2 Click **Delete**.
3 In the **Action** pane, click **OK**.

Removing systems from the Exceptions list

Use this task to remove detected systems from the **Exceptions** list. You might want to remove systems from the Exceptions list if you would like to start receiving detection information about it, or you know the system is no longer connected to your network.

This task can be performed from:	Getting there
Detected Systems Details page.	Go to **Network | Detected Systems**, click any detected system category in the **Overall System Status** monitor, and click any system.
Detected Systems page.	Go to **Network | Detected Systems** and click any detected system category in the **Overall System Status** monitor.

Task

For option definitions, click **?** on the page displaying the options.

1 Select the detected systems you want to remove from the **Exceptions** list.
From the **Detected Systems Details** page you can remove the systems you are viewing.
2 Click **Remove from Exceptions**.

Removing systems from the Rogue Sensor Blacklist

Use this task to remove detected systems from the **Rogue Sensor Blacklist**. Rogue System Detection prevents sensors from being installed on systems included in the blacklist. If you want to install a sensor on a system that has been blacklisted, you must remove the system from the list.

This task can be performed from:	Getting there
Rogue Sensor Blacklist Details page.	Go to **Network | Detected Systems**, click **View Blacklist** in the **Rogue System Sensor Status** monitor, and click any system.
Rogue Sensor Blacklist page.	Go to **Network | Detected Systems** and click **View Blacklist** in the **Rogue System Sensor Status** monitor.
Managed Systems for Subnet xxx.xxx.xxx.xxx page.	Go to **Network | Detected Systems**, click any subnet category in the **Subnet Status** monitor, then select any subnet and click **View Managed Systems.**
Systems Details page.	Go to **Systems | System Tree | Systems** and click any system.
Systems page.	Go to **Systems | System Tree**.

Task

For option definitions, click **?** on the page displaying the options.

1 Select the detected systems you want to remove from the **Rogue Sensor Blacklist**.

2 Click **Rogue Sensor Blacklist Remove**.
If the button is not visible, click **More Actions** and select **Rogue Sensor Blacklist Remove**.

Viewing detected systems and their details

Use this task to view detected systems and their details. You can view detected system details from any page that displays detected systems.

Task

For option definitions, click **?** on the page displaying the options.

1 Go to the **Network | Detected Systems**.

2 In the **Overall System Status** monitor, click any category to view the list of detected systems it contains, such as **Managed**. The **Detected Systems** page opens.

3 Click any detected system to view its details.

NOTE: The **System Details** page is different than the **Detected Systems Details** page. The **Detected Systems Details** page displays some information that is unique to Rogue System Detection.

Working with sensors

Use these tasks when working with sensors.

Tasks

- Changing the sensor-to-server port number
- Installing sensors
- Editing sensor descriptions
- Removing sensors

Changing the sensor-to-server port number

Use this task to change the sensor-to-server port number. You can change the port that the Rogue System Sensor uses to communicate with the ePO server.

NOTE: The sensor-to-server port number is specified in the ePO Sever Settings page, as well as in the Rogue System Detection policy settings. The port number specified in the Server Settings page can be changed only during installation of ePolicy Orchestrator. If you changed this port number during installation, you must also change it in the Rogue System Detection policy settings to allow sensors to communicate with the server.

Task

For option definitions, click **?** on the page displaying the options.

1 Go to **Systems | Policy Catalog**, then from the **Product** drop-down list select **Rogue System Detection 2.0.0**, and from the **Category** drop-down list select **General**. All created policies for Rogue System Detection appear in the details pane.

2 Locate the desired policy and click **Edit** in its row.

3 Under the **General** tab change the **Sensor-to-Server Communication Port** to the desired port number, then click **Save**.

Installing sensors

Use any of these tasks to deploy sensors to your network.

Tasks

- Installing sensors on specific systems
- Using queries and server tasks to install sensors
- Using client tasks to install sensors

Installing sensors on specific systems

Use this task to install sensors to specific systems on your network. This task creates a deployment task that installs the sensor to the selected systems, then performs an immediate agent wake-up call on them.

This task can be performed from:	Getting there
Managed Systems for Subnet xxx.xxx.xxx.xxx page.	Go to **Network | Detected Systems** and click any subnet category in the **Subnet Status** monitor, then select any subnet and click **View Managed Systems.**
Systems Details page.	Go to **Systems | System Tree | Systems** and click any system.
Systems page.	Go to **Systems | System Tree**.

Task

For option definitions, click **?** on the page displaying the options.

1 Select the systems where you want to install sensors, then click **Rogue Sensor Install**.

- In the **Systems Details** page, you can install the sensor only from the system you are viewing.
- In the **Managed Systems for Subnet xxx.xx.xx.x** page, select the systems where you want to install sensors.
- In the **Systems** page, select the desired group in the **System Tree** and select the systems where you want to install sensors.

NOTE: If the button is not visible, click **More Actions** and select **Rogue Sensor Install**.

2 In the **Action** pane, click **OK**.

Using queries and server tasks to install sensors

Use this task to create a query that can run as a server task action to install sensors on managed systems.

Task

For option definitions, click **?** on the page displaying the options.

1 Go to **Reporting | Queries**, then click **New Query** in the **Queries** pane.

2 On the **Result Type** page, select **Managed Systems** and click **Next**.
3 On the **Chart** page, from the **Display Results As**, click **Table**, then click **Next**.
4 From the **Available Columns** pane, click the types of information you want your query to return, then click **Next**.
5 Click the properties you want to filter with and specify the values for each, then click **Run**.
6 Click **Save** and specify the name of your query, and any notes, then click **Save** again.

TIP: McAfee recommends using a product specific prefix when naming your queries to keep them organized and make them easier to find. For example, RSD: QueryName.

7 Go to **Automation | Server Tasks**, then click **New Task**.
8 Name and describe the task and specify the Schedule status, then click **Next**.
9 From the drop-down list, select **Run Query**.
10 From the **Query** drop-down list, select the query you created. Then from the **Language** drop-down list, select the language in which to display the results.
11 Select **Rogue Sensor Install** as the action to take on the results, then click **Next**.
12 Specify the schedule for the task, then click **Next**.
13 Review the summary of the task, then click **Save**.

Using client tasks to install sensors

Use this task to create a client task that installs sensors to systems on your network.

Task

For option definitions, click **?** on the page displaying the options.

1 Go to **Systems | System Tree | Client Tasks** and select a group in the System Tree, then click **New Task**.
2 Type a name for the task you are creating, and any notes, then from the **Type** drop-down list select **Sensor Deployment** and click **Next**.
3 Select **Install** and click **Next**.
Select **Run at every policy enforcement** if needed.
4 Select whether the schedule is enabled and specify the schedule details, then click **Next**.
5 Review the summary and click **Save**.

Editing sensor descriptions

Use this task to edit sensor descriptions.

This task can be performed from:	Getting there
Rogue System Sensor Details page.	Go to **Network	Detected Systems**, click any sensor category in the **Rogue System Sensor Status** monitor, and click any sensor.
Rogue System Sensor page.	Go to **Network	Detected Systems** and click any sensor category in the **Rogue System Sensor Status** monitor.

Task

For option definitions, click **?** on the page displaying the options.

1 Select the system whose description you want to edit, and click **Edit Description**.

2 In the **Action** pane, type the description and click **OK**.

Removing sensors

Use any of these tasks to remove sensors from systems on your network.

Tasks

- Removing sensors from specific systems
- Using client tasks to remove sensors

Removing sensors from specific systems

Use this task to remove sensors from specific systems on your network. This task creates a deployment task that removes the sensor from the selected systems, then performs an immediate agent wake-up call on them.

This task can be performed from:	Getting there
Managed Systems for Subnet xxx.xxx.xxx.xxx page.	Go to **Network | Detected Systems** and click any subnet category in the **Subnet Status** monitor, then select any subnet and click **View Managed Systems**.
Systems Details page.	Go to **Systems | System Tree | Systems** and click any system.
Systems page.	Go to **Systems | System Tree**.

Task

For option definitions, click **?** on the page displaying the options.

1 Select the systems you want to remove sensors from, and click **Rogue Sensor Remove**.

- In the **Systems Details** page, you can remove the sensor from only the system you are viewing.
- In the **Managed Systems for Subnet xxx.xx.xx.x** page, select the systems you want to remove sensors from.
- In the **Systems** page, select the desired group in the **System Tree**, and select the systems you want to remove sensors from.

NOTE: If the **Rogue Sensor Remove** button is not visible, click **More Actions** and select **Rogue Sensor Remove**.

2 In the **Action** pane, click **OK**.

Using client tasks to remove sensors

Use this task to create a client task to remove sensors from systems on your network.

Task

For option definitions, click **?** on the page displaying the options.

1 Go to **Systems | System Tree | Client Tasks**, then select the desired group in the System Tree and click **New Task**.

2 Type a name for the task you are creating, and any notes, then from the **Type** drop-down list select **Sensor Deployment** and click **Next**.

3 Select **Remove** and click **Next**.
Select **Run at every policy enforcement** as needed.

4 Select whether the schedule is enabled and specify the schedule details, then click **Next**.

5 Review the summary and click **Save**.

Working with subnets

Use these tasks when working with subnets in Rogue System Detection.

Tasks

- Adding subnets
- Deleting subnets
- Ignoring subnets
- Including subnets
- Renaming subnets
- Viewing detected subnets and their details

Adding subnets

Use this task to add subnets to Rogue System Detection.

Task

For option definitions, click **?** on the page displaying the options.

1 Go to **Network | Detected Systems**, then in the **Subnet Status** monitor click **Add Subnet**.

2 Choose the method you want to use to add subnets and specify the subnets you want to add, then click **Import**.

Deleting subnets

Use this task to delete subnets from Rogue System Detection.

This task can be performed from:	Getting there
Detected Subnets Details page.	Go to **Network	Detected Systems** and click any category in the **Subnet Status** monitor, then click any system.
Detected Subnets page.	Go to **Network	Detected Systems** and click any category in the **Subnet Status** monitor.

Task

For option definitions, click **?** on the page displaying the options.

1 Select the subnets you want to delete and click **Delete**.

2 In the **Action** pane, click **OK**.

Ignoring subnets

Use this task to ignore subnets.

This task can be performed from:	Getting there
Detected Subnets Details page.	Go to **Network | Detected Systems** and click any category in the **Subnet Status** monitor, then click any system.
Detected Subnets page.	Go to **Network | Detected Systems** and click any category in the **Subnet Status** monitor.
Detected Systems homepage.	Go to **Network | Detected Systems**.

CAUTION: Ignoring a subnet deletes all detected interfaces associated with that subnet. All further detections on that subnet are also ignored.

Task

For option definitions, click **?** on the page displaying the options.

1 Select the subnets you want to ignore and click **Ignore**.

2 In the **Action** pane, click **OK**.
When ignoring a subnet on the **Detected Systems** homepage in the **Top 25 Subnets** list, a dialog box opens. Click **OK**.

Including subnets

Use this task to include subnets that have previously been ignored by Rogue System Detection.

Task

For option definitions, click **?** on the page displaying the options.

1 Go to **Reporting | Query**, and query ignored subnets. For more information on working with queries, see *Querying the Database.*

2 On the **Unsaved Queries** page, click **Include**.

3 In the **Actions** pane, click **OK**.

Renaming subnets

Use this task to rename subnets.

This task can be performed from:	Getting there
Detected Subnets Details page.	Go to **Network | Detected Systems** and click any subnet category in the **Subnet Status** monitor, then click any system.
Detected Subnets page.	Go to **Network | Detected Systems** and click any subnet category in the **Subnet Status** monitor.

Task

For option definitions, click **?** on the page displaying the options.

1 Select the subnet you want to rename and click **Rename**.

2 In the **Action** pane, type the new name for the subnet and click **OK**.

Viewing detected subnets and their details

Use this task to view detected subnets and their details. You can view detected subnets details from any page that displays detected subnets.

Task

For option definitions, click **?** on the page displaying the options.

1 Go to the **Network | Detected Systems**.

2 In the **Subnet Status** monitor, click any category to view the list of detected subnets it contains, such as **Covered**. The **Detected Subnets** page appears and displays the subnets in that category.

3 Click any detected subnet to view its details. The Detected Subnet Details page appears.

Rogue System Detection command-line options

You can run command-line options from the client system. You can start the sensor manually form the command-line instead of starting it as a Windows service. For example, you might want to do this if you are testing functionality, or to check the sensor version. The following table lists the run-time command-line options for the sensor.

Switch	Description
--console	Forces the sensor to run as a normal command-line executable; otherwise it must be run as an NT service.
--help	Prints the help screen and lists available command-line options.
--install	Registers the sensor with the Windows Service Control Manager.
--port	Overrides the ServerPort configuration setting in the registry that you specified during installation. NOTE: This parameter takes affect only when running in command-line mode, which also requires the --console command line switch. Sample syntax: sensor.exe --port "8081" --console
--server "[server name]" or "[IP address]"	Overrides the ServerName configuration setting in the registry that you specified during installation. NOTE: This parameter takes affect only when running in command-line mode, which also requires the --console command-line switch. Sample syntax: sensor.exe --server "MyServerName" --console
--uninstall	Unregisters the sensor with the Windows Service Control Manager.
--version	Prints the version of the sensor and exits.

Default Rogue System Detection queries

Rogue System Detection provides default queries that you can use to retrieve specific information from your network. These queries can be modified or duplicated in the same manner as other queries in ePolicy Orchestrator. You can also create custom queries, display query results in dashboard monitors, and add those dashboard monitors to the Dashboards section in ePolicy Orchestrator. For more information on using dashboards, see *Assessing Your Environment With Dashboards*.

Rogue System Detection query definitions

Query	Definition
RSD: Active Sensor Response (Last 24 Hours)	Returns the details of active sensors installed on your network in the last 24 hours, in pie chart format.
RSD: Passive Sensor Response (Last 24 Hours)	Returns the details of passive sensors installed on your network in the last 24 hours, in pie chart format.
RSD: Rogue Systems, By Domain (Last 7 Days)	Returns the details of systems detected on your network as rogue systems in the last seven days, grouped by domain, in table format.
RSD: Rogue Systems, By OS (Last 7 Days)	Returns the details of systems detected on your network as rogue systems in the last seven days, grouped by operating system, in pie chart format.
RSD: Rogue Systems, By OUI (Last 7 Days)	Returns the details systems detected on your network as rogue systems in the last seven days, grouped by grouped by organizationally unique identifier, in pie chart format.
RSD: Subnet Coverage	Returns the details of detected subnets on your network, in pie chart format.

Appendix: Maintaining ePolicy Orchestrator databases

Regardless of whether you use an MSDE or SQL database with ePolicy Orchestrator, your databases require regular maintenance over time. This ensures optimal performance and that the data in it is protected.

Depending on your deployment of ePolicy Orchestrator, plan on spending a few hours each week on regular database backups and maintenance. Many of the tasks in this section should be done on a regular basis, either weekly or daily. Some are only required at specific times, such as when there is a problem.

You can use a combination of tools to maintain ePolicy Orchestrator databases. You must use a slightly different set of tools depending on whether you are using a Microsoft Data Engine (MSDE) or SQL Server database as the ePolicy Orchestrator database. Note that you can use Microsoft SQL Server Enterprise Manager to maintain both MSDE and SQL Server databases.

Contents

- Performing daily or weekly database maintenance
- Backing up ePolicy Orchestrator databases regularly
- Changing SQL Server information
- Restoring ePolicy Orchestrator databases

Performing daily or weekly database maintenance

To keep your database from growing too large and to keep performance optimized, perform regular database maintenance on it. McAfee recommends doing this daily, if possible, or weekly at the very least. Performing this maintenance regularly can help keep the size of your database down and thereby improve database performance.

The task varies whether you are running an MSDE or SQL database.

Tasks

- Performing weekly maintenance of MSDE databases
- Performing regular maintenance of SQL Server databases

Performing weekly maintenance of MSDE databases

Use the SQLMAINT.EXE utility to regularly perform clean-up and maintenance on your MSDE database. By default, the SQLMAINT.EXE utility is installed in your MSDE installation folder on your server.

Run this utility at least once a week. You can use SQLMAINT.EXE command-prompt utility to perform routine database maintenance activities. It can be used to run DBCC checks, to dump a database and its transaction log, to update statistics, and to rebuild indexes.

The simple procedure below does not cover everything you can do with SQLMAINT to maintain your MSDE database, but rather the minimum you should do on your database each week. See the Microsoft web site for additional information on SQLMAINT and what it can do for your database.

Task

1 Type the following at the command prompt (the commands are case sensitive):

SQLMAINT -S <SERVER> -U <USER> -P <PASSWORD> -D <DATABASE> -RebldIdx 5 -RmUnusedSpace 50 10 -UpdOptiStats 15

Where <SERVER> is the name of the server, where <USER> and <PASSWORD> are the user name and password of the user account, and where <DATABASE> is the name of the database. The default database name is EPO_<SERVER> where <SERVER> is the name of the ePolicy Orchestrator server.

2 Press ENTER.

Performing regular maintenance of SQL Server databases

Use SQL Enterprise Manager to perform regular maintenance of your SQL database.

The tasks below do not cover everything you can do to maintain your SQL database in SQL Enterprise Manager. See your SQL documentation for details on what else you can do to maintain your database.

Backing up the transaction log is not compatible with simple recovery. If you have multiple databases with different recovery models, you can create separate database maintenance plans for each recovery model. In this way you can include a step to backup your transaction logs only on the databases that do not use the simple recovery mode.

Simple recovery mode is recommended because it prevents the transaction logs from swelling. In simple recovery, once a checkpoint is complete, the transaction logs for the time before the checkpoint are dropped from the active database. A checkpoint automatically occurs when the backup is made. We recommend having a database maintenance plan that performs a backup of the ePO database, together with "Simple Recovery". In this way, once a backup is successfully created, the portion of the transaction log in the active database will be dropped as it is no longer needed since a backup file exists.

Set the recovery model to simple. This is a one-time change to your SQL Server settings, and it is very important. While MSDE databases install with the simple recovery model by default, SQL Server installs using a different recovery model that doesn't allow the transaction log to be cleaned as easily. This can cause the log to swell in size.

NOTE: If you choose not to use simple recovery, then you need to regularly back up the transaction log.

See the SQL or MSDE documentation for setting the recovery model to simple.

Backing up ePolicy Orchestrator databases regularly

McAfee recommends that you back up ePolicy Orchestrator databases regularly to protect your data and guard against hardware and software failure. You may need to restore from a backup, such as if you ever need to reinstall the server.

How often you backup depends on how much of your data you are willing to lose. At a minimum, back up your database once a week, but you might want to backup daily if you have been making lots of changes to your deployment. You could also do daily backups as part of an automated nightly job. You can also spread the work by doing incremental daily backups and then a full weekly backup each week. Save the backup copy to a different server than the one hosting your live database--if your database server crashes you don't want to lose your backup too.

The process varies depending on whether you are backing up a SQL or MSDE database. To back up a SQL Server database, see your SQL Server documentation.

Tasks

- Backing up a SQL database--see your SQL documentation
- Backing up an MSDE database

Backing up a SQL database--see your SQL documentation

If you are using Microsoft SQL Server or SQL 2005 Express as the database, see the SQL Server product documentation.

Backing up an MSDE database

If you are using Microsoft Data Engine (MSDE) as the ePolicy Orchestrator database, you can use the Database Backup Utility (DBBAK.EXE) to back up and restore ePolicy Orchestrator MSDE databases on the database server.

TIP: The database backup utility works while the server service is running. However, McAfee recommends stopping the server service before beginning the backup.

You can back up and restore MSDE databases to the same path on the same database server using this utility. You cannot use it to change the location of the database

Task

1. Stop the **McAfee ePolicy Orchestrator 4.0 Server** service and ensure that the SQL Server (MSSQLSERVER) service is running. For instructions, see the operating system product documentation.
2. Close ePolicy Orchestrator.
3. Start the Database Backup Utility (DBBAK.EXE). The default location is:

   C:\PROGRAM FILES\MCAFEE\EPO
4. Type the **Database Server Name**.
5. Type the **Database Name**.
6. Select **NT Authentication** or **SQL Account**.

   If you selected **SQL Account**, type a user **Name** and **Password** for this database.
7. Type the **Backup File path**.

8 Click **Backup**.

9 Click **OK** when the backup process is done.

10 Start the **McAfee ePolicy Orchestrator 4.0 Server** service and ensure that the MSSQLSERVER service is running. For instructions, see the operating system product documentation.

Changing SQL Server information

Use this task to edit the SQL Server connection configuration details. This is useful to make changes to the user account information in ePolicy Orchestrator when you make changes to the SQL Server authentication modes in another program, for example, SQL Server Enterprise Manager. Do this if you need to use a privileged SQL user account for added network security.

You can use the page indicated below to adjust any database config file information that used to be done with the CFGNAIMS.EXE file.

Things to know about this page:

- Authentication — If the database is up, uses normal ePO user authentication and only a global administrator can access. If the database is down, a connection is required from the system running the server.
- The ePO server must be restarted for any configuration changes to take affect.
- As a last resort, you could always edit the config file by hand (${orion.server.home}/conf/orion/db.properties), putting in the plaintext password, starting the server and then using the config page to re-edit the db config, which will store the encrypted version of the passphrase.

Task

1 Go to this URL in ePolicy Orchestrator:

https://servername:port/core/config

2 In the **Configure Database Settings** page, scroll down and change the credentials as needed.

3 Click **OK** when done.

4 Restart the system to apply the changes.

Restoring ePolicy Orchestrator databases

If you have been backing up your database regularly as McAfee recommends, then restoring it is easy. You should not need to do this very often, or ever. Aside from software or hardware failure, you need to restore the database from a backup if you want to upgrade your server or database server hardware.

The process varies depending on whether you are backing up a SQL or MSDE database. To restore a SQL Server database, see your SQL Server documentation.

Tasks

- Restoring a SQL database--see your SQL documentation
- Restoring an MSDE database from a backup

Restoring a SQL database--see your SQL documentation

If you are using Microsoft SQL Server or SQL 2005 Express as the database, see the SQL Server product documentation.

Restoring an MSDE database from a backup

You can back up and restore MSDE databases to the same path on the same database server using this utility. You cannot use it to change the location of the database.

Task

1. Stop the **McAfee ePolicy Orchestrator 4.0 Server** service and ensure that the SQL Server (MSSQLSERVER) service is running. For instructions, see the operating system product documentation.
2. Close all ePolicy Orchestrator consoles and remote consoles.
3. Start the Database Backup Utility (DBBAK.EXE). The default location is:

   C:\PROGRAM FILES\MCAFEE\EPO
4. Type the **Database Server Name**.
5. Type the **Database Name**.
6. Select **NT Authentication** or **SQL Account**.

   If you selected **SQL Account**, type a user **Name** and **Password** for this database.
7. Type the **Backup File** path.
8. Click **Restore**.
9. Click **Yes** when asked whether you want to overwrite the entire ePolicy Orchestrator database.
10. Click **OK** when the restore process is done.
11. Start the **McAfee ePolicy Orchestrator 4.0 Server** service and ensure that the MSSQLSERVER service is running. For instructions, see the operating system product documentation.

Index

A

account credentials for agent installation package 73
accounts (See user accounts) 17
actions, Rogue System Detection
  events and 200
  events and automatic responses 201
  queries and installing sensors 207
Active Directory containers
  agent deployment and 74
  mapping to System Tree groups 57
Active Directory synchronization
  borders and 41
  deleting systems 43, 44
  duplicate entry handling 43
  integration with System Tree 43
  Synchronize Now action 43
  systems and structure 44
  tasks 43
  to System Tree structure 57
  types 44
administrator accounts (See user accounts) 17
administrators, global 39
agent
  about 14
  accessing multiple servers 89
  alien, on rogue systems 193
  command-line options 94
  configuring policies to use repositories 147
  defined 65
  deployment methods 72, 74
  enabling on existing McAfee products 78
  first call to server 47
  forcing calls to the server 79
  GUID and System Tree location 47
  inactive, on rogue systems 193
  maintenance 82
  McAfee Agent, ePO components 13
  notifications and event forwarding 156
  properties, viewing 85
  removal methods 81, 82
  removing from systems in query results 82
  Rogue System Detection configuration 198
  settings, viewing 87
  status determination 69
  tasks, running from managed systems 86
  uninstalling 82
  user interface 86
  version numbers, viewing 88
  wake-up calls 83
agent activity logs 69, 85
agent distribution
  deploying from ePolicy Orchestrator 74
  FRMINST.EXE command-line 81, 94
  methods 72, 74
agent distribution *(continued)*
  Novell NetWare servers 79
  requirements for deployment 74
  tasks 73
  using third-party deployment tools 79
  WebShield appliances 79
agent installation
  account credentials for 73
  CMDAGENT.EXE 94
  command-line options 94
  custom packages 73
  folder location 65
  forcing calls to server 79
  including on an image 78
  language packages 65
  login scripts 76
  manual 77
  network login scripts 76
  package, location of 66
  System Tree and 77
  uninstalling 82
  update packages 80
Agent Monitor 86
agent policy
  pages, options for 69
  settings, about 69
agent queries 180
agent upgrade 79, 80
agent-server communication
  about 66
  generating new ASSC keys 89
  secure communication keys (ASSC) 71
agent-to-server communication interval (ASCI)
  after agent setup 67
  global unique identifiers and 78
  recommended settings 66
aggregation (See notifications) 153
Apply Tag action 49
ASCI (See agent-to-server communication interval) 66
Audit Log 19, 172, 182

B

bandwidth
  considerations for event forwarding 28
  considerations for pull tasks 136
  distributed repositories and 97
  replication tasks and 137
  Rogue System Sensor and 191
  sensor-to-server traffic 191
best practices
  agent distribution 76
  agent-to-server communication interval 66
  deploying SuperAgents 67
  duplicating policies before assigning 117
  importing Active Directory containers 57

best practices *(continued)*
login scripts and agent installation 76
policy assignment locking 117
product deployment 134
SuperAgent wake-up calls 67
System Tree creation 51, 76
upgrading agents with ePO 80
borders (See System Tree organization) 41
branches
Change Branch action 150
Current 144, 148
deleting DAT and engine packages 151
Evaluation 150
manually moving packages between 150
Previous 138
types of, and repositories 99
broadcast segments and Rogue System Sensor 190

C

catch-all groups 47
Change Branch action 150
charts (See queries) 172
client tasks
about 117
creating and scheduling 129
deleting 129
editing settings for 129
installing RSD sensors 208
removing RSD sensors 209
working with 128
Command Agent tool (CMDAGENT.EXE) 67, 94
command-line options
agent 94
CMDAGENT.EXE 67, 79, 94
FRMINST.EXE 78, 81, 94
notifications and registered executables 160
rogue system detection 212
communication port, Rogue System Detection 196
communication to the server 191
compliance
compliant systems 193
configuring RSD settings 199
history, queries 181
summary, queries 181
components
ePO agent, about 65
ePO server, about 13
ePolicy Orchestrator, about 13
repositories, about 96
contacts
notifications and 18, 165
working with 26, 27
credentials
changing, on distributed repositories 112
criteria-based tags
applying 50, 51
sorting 55
Current branch
checking in update packages 148
defined 99
for updates 144

D

dashboards
active set 187
dashboards *(continued)*
chart-based queries and 184
configuring access and behavior 185
configuring for exported reports 28
configuring refresh frequency 185
creating 186
default monitors 184
granting permissions to 185
how they work 184
making active 186
making public 187
Rogue System Detection 193
selecting all in a set 187
DAT file updating
checking in manually 148
checking versions 149
considerations for creating tasks 135
daily task 149
deployment 133
from source sites 103
in master repository 99
scheduling a task 149
DAT files
deleting from repository 151
evaluating 150
repository branches 150
Data Roll-Up server task 174
databases
ePO, systems listed in 193
multi-server querying 173
ports and communication 18
public and personal queries 171
queries and retrieving data 170
registering servers for roll-up queries 174
DCOM 1.3, enabling ePO administration 74
deployment
checking in packages manually 138
global updating 141
installing products 140
package security 133
products and updates 133
supported packages 132
tasks 134
tasks, for managed systems 139
upgrading agents 80
detected systems
configuring policy settings 198
events and automatic responses 201
Exceptions list, adding to 202
Exceptions list, importing to 204
homepage 192
how Rogue System Sensor work 190
merging 204
merging and matching 192
removing from lists 204, 205
Rogue Sensor Blacklist, adding to 202
status monitors 192
viewing 206
working with 202
Detected Systems list, removing systems from 204
detections
configuring RSD policies 198
history, queries 181
per product query 183
settings for rogue systems 196
subnet status and rogue systems 195

devices
detected by Rogue System Sensor 190
DHCP servers
Rogue System Sensor and 191, 196
system and subnet reporting 190
Directory (See System Tree) 57
distributed repositories
about 97
adding to ePO 108
changing credentials on 112
creating and configuring 107
deleting 110
deleting SuperAgent repositories 107
editing existing 110
enabling folder sharing 109
ePO components 13
folder, creating 108
how agents select 138
limited bandwidth and 97
replicating packages to SuperAgent repositories 106
replicating to 145, 146
status queries 182
SuperAgent, tasks 105
types 98
unmanaged 98
unmanaged, copying content to 147
domain synchronization 41
duplicate entries in the System Tree 60

E

email addresses (See contacts) 18
email servers
configuring notifications 157
defining 28
enforcement (See policy enforcement) 126
engine updating
checking in manually 148
deployment packages 133
from source sites 103
in master repository 99
scheduling a task 149
engines
deleting from repository 151
repository branches 150
Evaluation branch
defined 99
using for new DATs and engine 150
events
contacts for notifications 18
determining which are forwarded 28
filtering, server settings 18
forwarding and notifications 156
forwarding, agent configuration and 69
notification rules for 168
events, Rogue System Detection
actions and 207
automatic responses, configuring 201
sensor settings 200
exceptions
Rogue System Blacklist 195
rogue system status 193
Exceptions list
adding systems 202
compared to Rogue Sensor Blacklist 195
events and automatic responses 201
Exceptions list *(continued)*
exporting 203
importing systems to 204
removing systems from 205
executables
configuring external commands 160
deleting 161
editing, notifications and 161
External Commands list 161
notifications and external commands 161
registered, adding 160
working with, for notifications 160
extension files
about 114
functionality added to managed products 114
installing 118
permission sets and installation 18
Rogue System Detection 189
version, viewing 23
external commands (See executables) 162

F

fallback sites
about 97
configuring 103
deleting 105
edit existing 105
switching to source 103
filters
Event Filtering settings 18
for server task log 30
query results 173
setting for notification rules 164
FRAMEPKG.EXE 66, 73, 94
FRMINST.EXE 94
FTP repositories
about 98
creating and configuring 107
editing 110
enabling folder sharing 109

G

geographic borders, advantages of 41
global administrators
about 17
assigning permission sets 17
creating groups 39
creating user accounts 23
permissions 17
global unique identifier (GUID) 47, 78
global updating
enabling 141
event forwarding and agent settings 69
process description 135
requirements 136
groups
catch-all 47
configuring criteria for sorting 55
creating manually 52
criteria-based 47
defined 39
deleting from System Tree 82
importing NT domains 59
moving systems manually 62
operating systems and 42

groups *(continued)*
pasting poilcy assignments to 128
policies, inheritance of 40
policy enforcement for a product 126
queries about 183
sorting criteria 55
sorting, automated 42
updating manually with NT domains 62
using IP address to define 41
viewing policy assignment 120
GUID (See global unique identifier) 78

H

HTTP repositories
about 98
creating and configuring 107
editing 110
enabling folder sharing 109

I

inactive systems, rogue system status 193
inheritance
and policy settings 116
broken, resetting 120
defined 40
viewing for policies 120
installation
Rogue System Sensor 207
Installation
Rogue System Sensor 207
intelligent filtering and Rogue System Sensor 190
Internet Explorer
configuring proxy settings 101
proxy settings and ePO 102
IP address
as grouping criteria 41
range, as sorting criteria 55
sorting 46
sorting criteria 51, 55
subnet mask, as sorting criteria 55

K

keys (See security keys) 88

L

LAN connections and geographical borders 41
language packages (See agent) 41
local distributed repositories 147
Locale IDs, settings for installation 94

M

Make Public action 178
managed systems
agent policy settings 69
agent wake-up calls 67
agent-server communication 66
deployment tasks for 140
Detected Systems list 204
Exceptions list 202
global updating and 97
installing products on 140
policy assignment 120
policy management on 115
managed systems *(continued)*
Rogue Sensor Blacklist 195, 202
rogue system status 193
roll-up querying 173
running an update task manually 86, 87
sorting, criteria-based 45
tasks for 140
viewing agent activity log 85
master repositories
about 96
checking in packages manually 148
communicating with source site 101
configuring proxy settings 102
ePO components 13
key pair for unsigned content 72
key pairs, using 91
pulling from source site 143, 144
replicating to distributed repositories 145, 146
updating with pull tasks 136
using Internet Explorer proxy settings 101
using replication tasks 137
McAfee Agent (see agent) 13
McAfee Default policy
frequently asked questions 130
McAfee Links, default monitor 184
McAfee recommendations
back up security keys 93
configure RSD sensor policies before deploying sensors 196
create a Roll Up Data server task 174
create new ASSC keys regularly 89
create System Tree segments with domain names or sorting filters 76
deploy agents when importing large domains 60
duplicate policies befote assignment 117
evaluate borders for organization 41
install multiple Rogue System Sensor per broadcast segment 191
schedule replication tasks 137
set agent policy prior to agent distribution 69
System Tree planning 40
use global updating 135
Microsoft Internet Information Services (IIS) 98
Microsoft Windows Resource Kit 54
monitors (See dashboards) 184
monitors, Rogue System Detection
overall system status 193
status monitors 192
My Default policy
frequently asked questions 130
MyAvert Threat Service, default monitor 184

N

NAP files (See extension files) 114
NETDOM.EXE utility, creating a text file 54
network bandwidth (See System Tree organization) 41
network login scripts (See agent installation) 76
network traffic
bandwidth 191
Rogue System Sensor and 190
Notification Log
configuring 166
purging notifications 167
viewing 166, 167
Notification Rule Builder wizard 165
notification rules
creating and editing 163

notification rules *(continued)*
defaults 155
Description page 163
for products and components 168
importing .MIB files 159
setting filters for 164
setting thresholds 164
notifications
assigning permissions 157
configuring 157, 160, 165
contacts for 18, 165
event forwarding 156, 157
event forwarding and agent settings 69
external commands, working with 161, 162
frequently asked questions 168
history of, viewing 166
how they work 153
planning 155
recipients 153
registered executables, working with 160, 161
rules that trigger 165
SNMP servers 158, 159
System Tree scenarios 153
throttling and aggregation 153
Novell NetWare servers, agent deployment and 79
NT domains
importing to manually created groups 59
integration with System Tree 43
synchronization 45, 59
updating synchronized groups 62

O

operating systems
filters for notification rule 164
grouping 42
legacy systems (Windows 95, Windows 98) 42
Microsoft Windows XP Service Pack 2 73
Rogue System Detection and 190
Rogue System Sensor and 190
Windows 95 74
Windows 98 74
Windows ME 74
Windows XP Home 74
overall system status, Rogue System Detection 193

P

packages
checking in manually 138
configuring deployment task 140
deploying updates with tasks 142
moving between branches in repository 150
security for 71, 133
passwords
changing on user accounts 24
installing agents, command-line options 94
logging on to ePO servers 22
permission sets
at product installation 18
creating for user accounts 25
extensions and 18
how they work 17
rogue system detection 197
working with 24, 25, 26
permissions
assigning for notifications 157
permissions *(continued)*
for queries 171
global administrator 17
to dashboards 185
policies
about 115
assigning and managing 123
broken inheritance, resetting 120
categories 115
changing the owner 123
controlling on Policy Catalog page 121, 122, 123
enforcing 87
frequently asked questions 130
group inheritance, viewing 120
how they are applied to systems 116
importing and exporting 116, 124, 125
inheritance 116
ownership 117, 119
settings, viewing 119
sharing between ePO servers 124
update settings 87
verifying changes 85
viewing 115, 118
working with Policy Catalog 121
policies, Rogue System Detection
about 196
compliance settings 199
configuring 198
considerations 196
matching settings 199
sensor-to-server port 206
policy assignment
copying and pasting 127, 128
disabled enforcement, viewing 119
group, assigning to 125
locking 117
Policy Catalog 116
systems, assigning to 125, 126
viewing 118, 120
Policy Catalog
page, viewing 115
working with 121
policy enforcement
enabling and disabling 126
for a product 126
viewing assignments where disabled 119
when policies are enforced 116
policy management
using groups 39
working with client tasks 128
ports
communication, working with 29, 88
reconfiguring 88
RSD sensor-to-server port 196, 206
server settings 18
server settings and communication 18
Previous branch
defined 99
moving DAT and engine packges to 151
saving package versions 138
product deployment packages
checking in 138
checking in manually 148
security and package signing 133
supported packages 132
updates 133

product installation
configuring deployment tasks 140
extensions and permission sets 18
installing extension files 118
Locale ID settings 94
product updates
checking in packages manually 138
deploying 133
legacy support 133
package signing and security 133
process description 134
source sites and 97
supported package types 132
product version number, viewing 88
properties
agent, viewing from the console 85
full and minimal for systems 70
sending to ePO server 86
verifying policy changes 85
proxy settings
configuring ePO for Internet Explorer 102
configuring for master repository 102
Internet Explorer, using for master repository 101
pull tasks
considerations for scheduling 136
deploying updates 142
Pull Now task, initiating 144
server task log 138
updating master repository 136, 143

Q

queries
about 170
actions on results 170
chart types 172
contacts 18
custom, creating 175
defaults 180
duplicating 178
exported as reports 171
exporting to XML file 179
filters 173
importing from a server 179
making personal queries public 178
My Queries list 171
permissions 171
preparing for roll-up queries 174
public and personal 171
Public Queries list 171
registering ePO servers 174
removing agents in results of 82
report formats 171
results as dashboard monitors 171
results as tables 173
roll-up from multiple servers 173
running existing 176
scheduled 176
using results to exclude tags on systems 49
queries, Rogue System Detection
installing sensors 207
Query Builder wizard
about 172
creating custom queries 175
result types 172
query names
Agent Communication Summary 180
Agent Version Summary 180
Compliance History 181
Compliance Summary 181
Detection History 181
Distributed Repository Status 182
Failed Logon Attempts 182
Failed User Actions in ePO Console 182
Managed Systems History 182
Systems per Top-Level Group 183
Systems Tagged as Server 183
Todays Detections per Product 183
Quick System Search, default monitor 184

R

registered executables (See executables) 160
Replicate Now task 146
replication tasks
copying contents of master repository 145
deploying updates 142
full vs. incremental 137
Replicate Now task from master repository 146
scheduling repository replication 145
server task log 138
updating master repository 137
reports
configuring template and location for 28
exported data 21
exported query results 171
formats 21, 171
repositories
branches 99, 150
creating SuperAgent repository 106
how they work together 100
importing from repository list files 111
master, configuring proxy setttings for 102
replication and selection of 137
replication tasks 146
scheduling a pull task 143
scheduling a replication task 145
source site 97, 144
types of 96
unnmanaged, copying content to 147
repository list files
about 99
adding distributed repository to 108
exporting to 110, 111
importing from 111, 112
SITELIST.XML, uses for 99
working with 110
Rogue Sensor Blacklist
about 195
adding systems 202
removing systems from 205
Rogue System Detection
about 189
agents and 198
compliance settings 199
configuring server settings 199
deploying sensors 207
events, configuring responses 201
operating system support 190
policy configuration 198
policy settings 196

Rogue System Detection *(continued)*
sensor blacklist 195
sensor settings 200
sensor-to-server communication port 196
setting up 198
status and states 192
working with subnets 210, 211, 212
Rogue System Sensor
about 190
active, configuring 200
blacklist 195
data gathering 191
installation 207
installing 207, 208
operating systems and 190
removing 209
RSD settings, configuring 200
sensor-to-server port, changing 206
status and sensor states 194
traffic and intelligent filtering 190
working with 206
rogue systems
about 189
system status 193
Top 25 Subnets list 195
roll-up queries (See queries) 173
rules
configuring contacts for notifications 165
defaults for notifications 155
setting up for notifications, SNMP servers 159
Run Tag Criteria action 49

S

scheduling
applying criteria-based tags 51
client tasks 129
Repository Pull task 143
Repository Replication task 145
security keys
agent-server communication 71
backing up and restoring 93
deleting ASSC 91
exporting to agents 89
for content from other repositories 72
generating and using 89
making a key pair the master 90
private and public 72
server settings 18
systems using one ASSC key 90
using key pairs for servers 88, 89
working with 88
sensor-to-server port 196, 206
server settings
ASSC keys and 89
configuring Rogue System Detection 199
global updating 141
Internet Explorer 101
notifications 155
ports and communication 18
proxy, and master repositories 96
types of 18
working with 27
Server Task Builder wizard 51
server task log
about 138
server task log *(continued)*
filtering for recent activity 30
Pull Now task 144
purging 31
Replicate Now task 146
reviewing status of tasks 30
working with 29
server tasks
Data Roll-Up 174
defining email servers 28
installing Rogue System Sensor 207
log file, purging 31
Repository Pull, scheduled 143
Repository Replication 145
scheduling a query 176
Synchronize Domain/AD 43
types and definitions 19
servers
ePO server, components 13
importing and exporting policies 116
importing and exporting queries 179
importing policies from 125
introduction 13
license information, viewing 23
logging on and off 22, 23
master repository key pair 72
queries about 182, 183
registering, for queries 174
roll-up queries 174
server task log, about 138
settings and controlling behavior 18
sharing policies 124
SNMP, and notifications 158, 159
tasks, scheduling repository replication 145
using contents from other servers 92
using security key pairs 89
viewing version number 23
sites
deleting source or fallback 105
editing existing 105
fallback 97, 103
switching source and fallback 103
SNMP servers (See notifications) 158, 159
Sort Now action 45
sorting criteria
configuring 55
for groups 55
groups, automated 42
IP address 46
IP address-based 55
sorting systems into groups 45
tag-based 42, 47, 55
source sites
about 97
configuring 103
creating source sites 104
deleting 105
editing existing 105
fallback 97
importing from SITEMGR.XML 112
product updates and 97
pulling from 143, 144
switching to fallback 103
update packages and 133
SPIPE 66
SQL servers (See databases) 41

status monitors
detected systems 192
subgroups
and policy management 59
criteria-based 47
subnets
active RSD sensors, configuring duration 200
events and automatic responses 201
in Rogue System Detection 210, 211, 212
status, Rogue System Detection 195
Top 25 Subnets list 195
subnets, as grouping criteria 41
SuperAgent repositories
about 98
creating 106
deleting 107
global updating requirements 136
replicating packages to 106
tasks 105
SuperAgents
as repositories 65
distributed repositories 98
wake-up calls 67, 83
wake-up calls to System Tree groups 83
synchronization
Active Directory and 44
defaults 48
deploying agents automatically 44
excluding Active Directory containers 44
importing systems 44
NT domains 45
preventing duplicate entries 44
scheduling 61
Synchronize Now action 43
systems and structures 44
system status
monitors 192
Rogue System Detection 193
System Tree
access requirements 40
assigning policies to a group 125
child groups and inheritance 40
creation, automated 41
criteria-based sorting 45
defined 39
deleting systems from 39, 81
groups and manual wake-up calls 83
My Organization level 39, 40
parent groups and inheritance 40
permission sets 40
populating groups 51
removing agents 81, 82
System Tree organization
borders in your network 41
creating groups 51
duplicate entries 60
importing Active Directory containers 57
importing systems and groups 53, 54
mapping groups to Active Directory containers 57
moving systems to groups manually 62
network bandwidth 41
operating systems 42
planning considerations 40
text files, importing systems and groups 54
using subgroups 59
System Tree sorting
default settings 48
enabling 56
on agent-server communication 46
ordering subgroups 47
server and system settings 18, 46
sort systems once 46
tag-based criteria 47
System Tree synchronization
Active Directory integration 43
NT domain integration 43
scheduling 61
to Active Directory structure 57
systems
assigning policies to 125, 126
pasting policy assignments to 128
policy enforcement for a product 126
properties, full and minimal 70
sorting into groups 56
viewing policy assignment 120

T

tables and charts
exported as reports 21
report formats 21
Tag Builder wizard 49
Tag Catalog 49
tag-based sorting criteria 42, 47
tags
applying 50, 51
creating with Tag Builder wizard 49
criteria-based 43, 45
criteria-based sorting 55
defined 42
excluding systems from automatic tagging 49
group sorting criteria 42
manual application of 50
permissions for 42
types 43
without criteria 43
working with 48
Test Sort action 45
third-party distribution tools 79
throttling (See notifications) 153
troubleshooting
agent activity logs 69
product deployment 134
verifying properties of agent and products 85
viewing product and agent version numbers 88

U

UNC share repositories
about 98
creating and configuring 107
editing 110
enabling folder sharing 109
unmanaged repositories 98
updates
agent installation packages 80
checking in manually 138
client tasks 134
considerations for creating tasks 135
deploying packages with tasks 142
deployment packages 133
package signing and security 133

updates *(continued)*
packages and dependencies 133
running tasks manually 86, 87
scheduling an update task 149
source sites and 97
upgrading agents 80
updating
agents, with login scripts or manual installation 80
automatically, with global updating 141
DATs and engine 133
deployment tasks 134
global, process 135
manually 86, 87
master repository with pull tasks 143
process description 134
Pull Now task to update master repository 144
scheduling an update task 149
user accounts
about 17
changing passwords 24
creating 23
creating permission sets for 25
user accounts *(continued)*
permission sets and 17
working with 23, 24
user interface, agent 86
utilities
NETDOM.EXE, creating a text file 54

V

VCREDIST.EXE, enabling ePO administration 74
VPN connections and geographical borders 41

W

wake-up calls
manual 83
scheduled 84
SuperAgents and 67, 83
to System Tree groups 83
when to send 67
WAN connections and geographical borders 41
WebShield appliances, agent deployment and 79
Windows (See operating systems) 74